FortiOS Handbook

What's New for FortiOS 5.0

FortiOS Handbook - What's New for FortiOS 5.0 (Updated for Patch 6)

March 11, 2014

01-502-117003-20130403

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
Video Tutorials	video.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

New features in FortiOS 5.0 Patch 2 54

Security Features 62

Change Log

Date	Change Description
2014-03-11	Updated “SSH inspection” on page 80.
2014-01-20	Added “New features in FortiOS 5.0 Patch 6” on page 15.
2013-11-07	Added “Limiting access for unauthenticated users” on page 24.
2013-11-01	Added “New features in FortiOS 5.0 Patch 5” on page 18. Updated “Viewing client reputation results” on page 109. Added “Converting compact log format” on page 142. Edits throughout the document to bring the content up to date for patch 5.
2013-09-17	Removed FortiCloud chapter (moved to *Installation and System Administration*).
2013-08-21	Changed Figure 7 on page 33 (the Wireless Health Monitor).
2013-08-14	Added “New features in FortiOS 5.0 Patch 4” on page 32. Divided “Advanced Persistent Threat (APT) protection” into new section, “FortiSandbox” on page 62, and “Botnet and phishing protection” on page 63. Edits throughout the document to bring the content up to date for patch 4.
2013-06-24	Added “New features in FortiOS 5.0 Patch 3” on page 42. Removed Endpoint Control chapter. Renamed UTM chapter to Security Features. Added section “Exempting IP addresses from IPS” on page 68. Replaced the Viewing and hiding features in the web-based manager section with “Feature Select” on page 168. Edits throughout the document to bring the content up to date for patch 3.
2013-04-03	Added more information to “Changes to logging in security policies” on page 54. Added section “The SIP ALG can receive SIP traffic on multiple TCP and UDP ports” on page 59. Added section “IPv6 PIM sparse mode multicast routing” on page 59. Added section “Wireless RADIUS-Based MAC Authentication” on page 59. Section renamed and more information added “FortiGate Session Life Support Protocol (FGSP)” on page 179.

Date	Change Description
2013-03-18	Removed the Endpoint Control Extensions: FortiClient registration and endpoint profile management section from "Authentication: users and devices" on page 83. Added "New features in FortiOS 5.0 Patch 2" on page 54. Added "Endpoint Control" on page 21. Changes to "Client Reputation" on page 106. Changes to "Advanced Persistent Threat (APT) protection" on page 30. Edits throughout the document to bring the content up to date for patch 2.
2013-02-19	Added info about platform support to the following sections: • "SSO with Windows AD or Novell" on page 89 • "Citrix Agent support for Single Sign On" on page 90
2013-01-17	Correction to "Advanced Persistent Threat (APT) protection" on page 30 about support for proxy and flow-based botnet protection.
2013-01-16	Changes have been made throughout the document to update it for FortiOS 5.0 patch 1. Here are some highlights: • Changes to "WAN optimization and Web Caching" on page 155 to remove examples as they are now included in WAN Optimization, Web Cache, Explicit Proxy, and WCCP for FortiOS 5.0. Also added information about SSL web caching changes for FortiOS 5.0 • Updated "Config features" on page 138. • "DLP watermarking" on page 77 updated with information about the Fortinet watermarking client. • "Client Reputation" on page 106 updated to reflect changes to this feature. • "SSL and SSH inspection" on page 153 updated to describe new SSL/SSH inspection profiles. • "New default SSL VPN portals" on page 176 lists the new portals. • "New HA mode: Fortinet redundant UTM protocol (FRUP)" on page 180
2012-11-21	Corrections to "Identifying Skype sessions" on page 173.
2012-11-14	New section "New SIP ALG features" on page 73. Added more info about WAN optimization and UTM to "WAN optimization and Web Caching" on page 155
2012-11-02	New FortiOS 5.0 release.

Chapter 1 What's New for FortiOS 5.0

This FortiOS Handbook chapter contains the following sections:

- New features in FortiOS 5.0 Patch 5 highlights some of the changes in FortiOS 5.0 Patch 5.
- New features in FortiOS 5.0 Patch 4 highlights some of the changes in FortiOS 5.0 Patch 4.
- New features in FortiOS 5.0 Patch 3 highlights some of the changes in FortiOS 5.0 Patch 3.
- New features in FortiOS 5.0 Patch 2 highlights some of the changes in FortiOS 5.0 Patch 2.
- Security Features describes new Security features.
- Authentication: users and devices describes what's new for FortiOS user authentication and device management.
- FortiOS and BYOD outlines how to configure FortiOS device identification and BYOD protection features.
- Client Reputation introduces the new client reputation feature.
- Wireless describes new wireless features.
- IPv6 describes new IPv6 features and how to configure many of them.
- Logging and reporting summarizes new FortiOS 5.0 logging and reporting features.
- Firewall describes the firewall features new to FortiOS 5.0.
- WAN optimization and Web Caching provides an overview and some examples that show how you need to change your FortiOS 4.3 WAN optimization configuration to work with FortiOS 5.0 WAN optimization, which is now policy-based.
- Usability enhancements describes some enhancements that make the web-based manager easier to use and more effective.
- SSL VPN describes some new SSL VPN features
- Other new features lists other new features in FortiOS 5.0.

New features in FortiOS 5.0 Patch 6

This chapter provides a brief introduction to the following features that were added to Patch 6 of FortiOS 5.0. See the release notes for a complete list of new features/resolved issues in this release.

Endpoint Control Daemon Improvement

Endpoint Control has been improved in several ways:

- The maximum limit of FortiClient registration licence has been increased from 8000 to 16000.
- The intervals between KeepAlive messages are now configurable on the FortiGate unit, so that the the interval value can be adjusted to get a tradeoff between accuracy and the FortGate workload. This value can be configured in the CLI:

  `set forticlient-keepalive-interval <interval>` (interval measured in seconds).
- The intervals between two system update messages can be configured through the CLI:

  `set forticlient-sys-update-interval <interval>` (interval measured in minutes).
- KeepAlive timestamps are now be stored use a in-momery avl tree structure, in order to decrease the the number of CMDB savings.
- A mixed TCP/UDP mechanism now handles the registration sync.
- FortiClient registration information is stored using a hard disk instead of flash disk.

IPS Hardware Acceleration

New CLI commands have been added for configuring IPS hardware acceleration, replacing the previous `set hardware-accel-mode` command, to provide finer control over the settings. There are now two settings that can be chosen, one for the network processor and one for the content processor.

Network processor acceleration can be disabled or set to enable basic acceleration. Content processor acceleration can be disabled or enabled for either basic or advanced acceleration.

Syntax

```
config ips global
   set np-accel-mode {none | basic}
   set cp-accel-mode {none | basic | advanced}
end
```

802.11g Protection Mode

802.11g Protection Mode can now be enabled on managed FortiAP to avoid interference from 802.11b signals. Protection Mode can be set for RTS and CTS protection, or just for CTS.

Syntax

```
config wireless-controller wtp-profile
   edit <name>
      config radio-1
         set protection-mode {ctsonly | disable | rtscts}
      end
   end
end
```

Miglogd Child Processes

The number of miglogd child processes can now be configured directly through CLI to a value between 0-15, in order to keep up with logging requirements. The default number of child processes is 8.

Log messages are not lost if the number of child processes is decreased.

Syntax

```
config system global
   set miglogd-children <integer>
end
```

Increasing the number of child processes may affect a FortiGate unit's performance.

IPv6 in CRL/SCEP

IPv6 is now supported for all certificate revocation list (CRL) and Simple Certificate Enrollment Protocol (SCEP) features.

Extended IPS Database for D-series Desktop Models

The extended IPS database has been added for FortiGate D-series Desktop models. The extended database is disabled by default, but can be enabled in the CLI.

Syntax

```
config ips global
  set database extended
end
```

Enabling the extended IPS database may affect the performance of a FortiGate unit.

Logging Options for 3000 and 5000 Series Models

To increase stability of the 3000 series and 5000 series FortiGate models, the following changes have been made:

- Disk logging is disabled by default, but can be enabled through the CLI.
- When disk logging is disabled, it will not appear disk logging as an option on these models.

The default logging method for these models is now memory logging, which has been reintroduced as an option.

Wireless Controller on FortiGate-30D

The Wireless Controller has been added to the FortiGate-30D, which is now able to manage a maximum of 2 FortiAP units.

By default, this feature is only available through the CLI. To enable the Wireless Controller menu in the web-based manager support, enter the following command in the CLI:

```
config system global
  set gui-wireless-controller enable
end
```

When enabled, the default WiFi menu will be replaced by the full Wireless Controller menu in the web-based manager.

You can also use the command `set gui-ap-profile enable` to enable FortiAP and WIDS profiles.

New features in FortiOS 5.0 Patch 5

This chapter provides a brief introduction to the following features that were added to Patch 5 of FortiOS 5.0. See the release notes for a complete list of new features in this release.

Improvements to Endpoint Control

There have been several improvements made to Endpoint Control.

New menu options

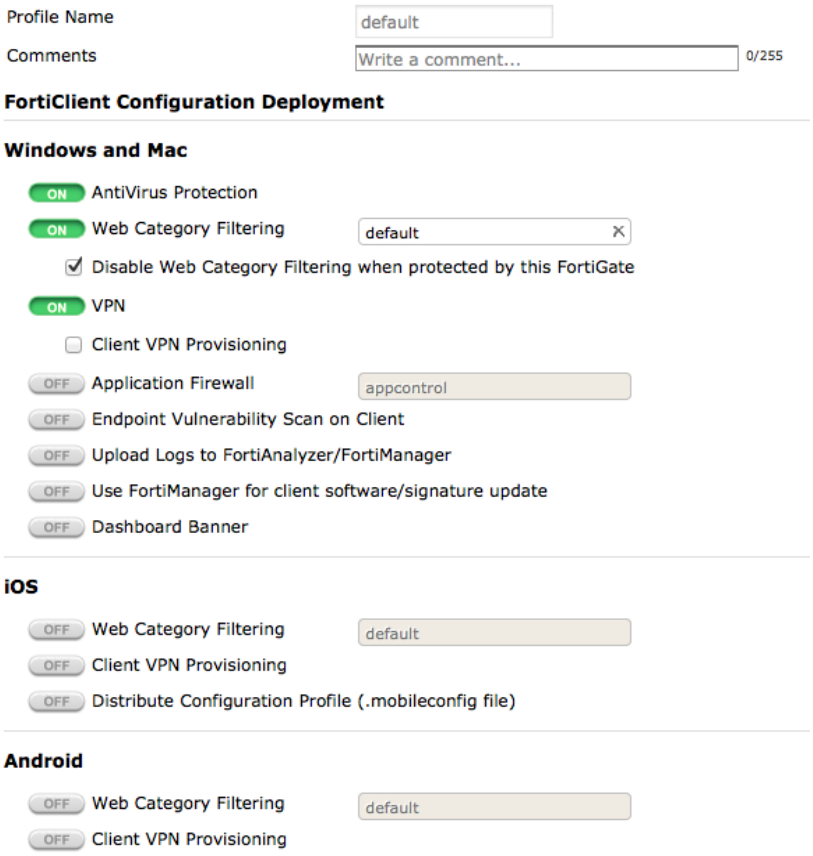
Endpoint Control now has its own menu, which can be found at *User & Device* > *Endpoint Protection.* This menu contains options for creating FortiClient profiles.

Default profile

A default FortiClient profile has been added that enables AntiVirus, Web Filtering, and VPN for Windows and Mac. All other features are disabled.

The profile creation screen has also been simplified to allow for easier configuration.

Figure 1: The default FortiClient profile



FortiClient Monitor

The FortiClient Monitor displays a variety of information about FortiClient users, including current status, device type, and FortiClient version. It can be found by going to *User & Device* > *Monitor* > *FortiClient*.

FortiAP LAN port support

New functions are now available for FortiAP models that have LAN ports (currently the 11C, 14C, and 28C). The LAN port(s) can now be bridged to either an SSID or to the FortiAP unit's WAN port (bridging to the WAN port is the default setting).

LAN port bridging can be done with FortiAP units in either Bridge or Tunnel mode.

Bridging with the FortiAP's SSID(s)

Bridging the LAN port with the FortiAP's SSID(s) allows combines traffic from both sources to provide a single broadcast domain for the wired and wireless users.

This configuration has the following features:

- The IP addresses for LAN clients come from the DHCP server that is serving the wireless clients.
- Traffic from LAN clients is bridged to the VLAN used by the SSID to send traffic to the controller.
- Wireless and LAN clients are on the same network and can communicate locally, via the FortiAP.

Bridging with the WAN port

Bridging the LAN port with the WAN port allows the FortiAP unit to be used as a hub which is also an access point.

This configuration has the following features:

- The IP addresses for LAN clients come from the WAN directly and will typically be in the same range as the AP itself.
- All LAN client traffic is bridged directly to the WAN interface.
- Communication between wireless and LAN clients can only occur if a policy on the FortiGate unit allows it.

Configuring bridging

A FortiAP LAN port can be configured to bridge with an SSID from either the web-based manager or the CLI.

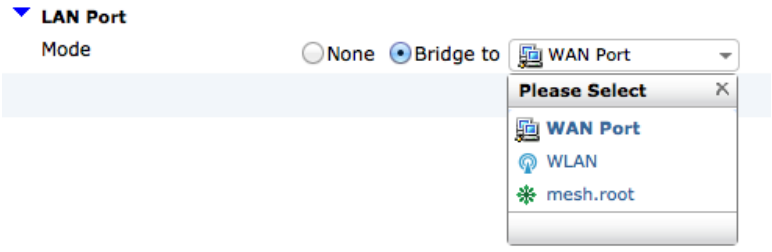
Using the web-based manager

1. Go to *WiFi Controller* > *WiFi Network* > *Custom AP Profiles.*

On FortiGate models 100D, 200D, 240D, 600C, 800C, and 1000C, go to *WiFi & Switch Controller* > *WiFi Network* > *Custom AP Profiles.*

2. Create a new custom profile or edit the default profile for your FortiAP model.
3. Under *LAN Port*, change *Mode* to *Bridge to* and select the appropriate option.
4. Select *OK.*

Figure 2: Configuring bridging using the web-based manager



Bridging can also be set up configured on a specific FortiAP unit, rather than through the use of an AP profile by going to *WiFi Controller* > *Managed Devices* > *Managed FortiAPs.*

On FortiGate models 100D, 200D, 240D, 600C, 800C, and 1000C, go to *WiFi & Switch Controller* > *Managed Devices* > *Managed FortiAPs.*

Using the CLI

In the example below, two ports on a FortiAP-28C are configured, with port 1 bridged to the WAN port and port 2 bridged to the SSID(s):

```
config wireless-controller wtp-profile
  edit FAP28C-default
    config lan
      set port1-mode bridge-to-wan
      set port2-mode bridge-to-ssid
    end
  end
end
```

Bridging can also be set up configured on a specific FortiAP unit, rather than through the use of an AP profile:

```
config wireless-controller wtp
  edit FAP28C0123456789
    config lan
      set port1-mode bridge-to-wan
      set port2-mode bridge-to-ssid
    end
  end
end
```

Restrictions

- While the FortiAP-14C has four physical LAN ports, these ports must share the same configuration.
- Any host connected to a LAN port will be taken as authenticated.
- The use of dynamic VLANs for the host behind LAN port is not supported.
- RADIUS MAC authentication for the host behind LAN port is not supported.

Automatically allowing basic applications

Application control profiles can now be configured from the CLI to allow basic, commonly used applications to go through without having to separately configure the profile each application. This is useful when you wish to control the traffic to an entire category of applications without affecting the traffic for basic applications that are required on a daily basis.

For example, an application sensor that blocks the Category "Network.Service" would normally also block DNS service, causing Internet service issues. Using the new command, DNS can now be allowed, eliminating this issue while still blocking other applications within the category.

Basic traffic can also be allowed for ICMP, generic HTTP web browsing, and generic SSL communication.

Syntax

```
config application list
  edit appcontrol
    set options allow-dns allow-icmp allow-http allow-ssl
end
```

DNS is set to be allowed be default for all application control profiles, while the other settings must be enabled to take effect.

Pre-authorizing a FortiAP unit

Users can now pre-authorize a FortiAP unit by before connecting the unit to the FortiGate unit. To pre-authorize a FortiAP unit, do the following:

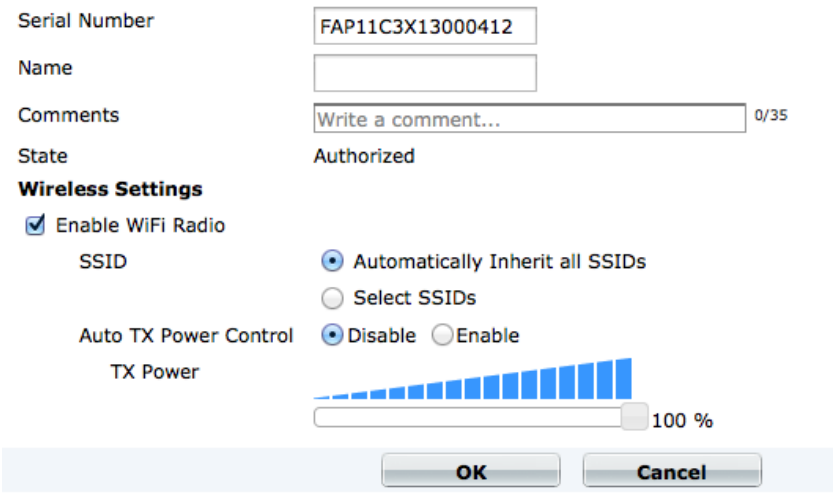
1. Go to *WiFi Controller* > *Managed Access Points* > *Managed FortiAPs* and select *Create New*.

On FortiGate models 100D, 200D, 240D, 600C, 800C, and 1000C, go to *WiFi & Switch Controller* > *Managed Devices* > *Managed FortiAPs*

2. Enter the serial number of the FortiAP unit.
3. Configure the *Wireless Settings* as required.
4. Select *OK*.

The new FortiAP now appear on the Managed FortiAPs list as authorized but off-line. The FortiAP unit can now connect to the FortiGate unit.

Figure 3: Pre-authorizing a FortiAP unit



If the FortiAP unit will be connecting directly to one of the FortiGate unit's ports, the port will still need to have its *Addressing mode* set to *Dedicate to FortiAP*.

Preventing IP fragmentation of packets in CAPWAP tunnels

A common problem with controller-based WiFi networks is reduced performance due to IP fragmentation of the packets in the CAPWAP tunnel.

Fragmentation can occur because of CAPWAP tunnel overhead increasing packet size. If the original wireless client packets are close to the maximum transmission unit (MTU) size for the network (usually 1500 bytes for Ethernet networks unless jumbo frames are used) the resulting CAPWAP packets may be larger than the MTU, causing the packets to be fragmented. Fragmenting packets can result in data loss, jitter, and decreased throughput.

The FortiOS/FortiAP solution to this problem is to cause wireless clients to send smaller packets to FortiAP devices, resulting in1500-byte CAPWAP packets and no fragmentation. The following options configure CAPWAP IP fragmentation control:

```
config wireless-controller wtp
  edit new-wtp
    set ip-fragment-preventing {tcp-mss-adjust | icmp-unreachable}
    set tun-mtu-uplink {0 | 576 | 1500}
    set tun-mtu-downlink {0 | 576 | 1500}
  end
end
```

By default, `tcp-mss-adjust` is enabled, `icmp-unreachable` is disabled, and `tun-mtu-uplink` and `tun-mtu-downlink` are set to 0.

To set `tun-mtu-uplink` and `tun-mtu-downlink`, use the default TCP MTU value of 1500. This default configuration prevents packet fragmentation because the FortiAP unit limits the size of TCP packets received from wireless clients so the packets don't have to be fragmented before CAPWAP encapsulation.

The `tcp-mss-adjust` option causes the FortiAP unit to limit the maximum segment size (MSS) of TCP packets sent by wireless clients. The FortiAP does this by adding a reduced MSS value to the SYN packets sent by the FortiAP unit when negotiating with a wireless client to establish a session. This results in the wireless client sending packets that are smaller than the `tun-mtu-uplink` setting, so that when the CAPWAP headers are added, the CAPWAP packets have an MTU that matches the `tun-mtu-uplink` size.

The `icmp-unreachable` option affects all traffic (UDP and TCP) between wireless clients and the FortiAP unit. This option causes the FortiAP unit to drop packets that have the "Don't Fragment" bit set in their IP header and that are large enough to cause fragmentation and then send an ICMP packet -- type 3 "ICMP Destination unreachable" with code 4 "Fragmentation Needed and Don't Fragment was Set" back to the wireless controller. This should cause the wireless client to send smaller TCP and UDP packets.

Limiting access for unauthenticated users

When configuring User Identity policies, if you select the option *Skip this policy for unauthenticated user* the policy will only apply to users who have already authenticated with the FortiGate unit. This feature is intended for networks with two kinds of users:

- Single sign-on users who have authenticated when their devices connected to their network
- Other users who do not authenticate with the network so are “unauthenticated”

Sessions from authenticated users can match this policy and sessions from unauthenticated users will skip this policy and potentially be matched with policies further down the policy list. Typically, you would arrange a policy with *Skip this policy for unauthenticated user* at the top of a policy list.

You can also use the following CLI command to enable skipping policies for unauthenticated users:

```
config firewall policy
  edit <id>
    set identity-based enable
    set fall-through-unauthenticated enable
    next
```

Use case - allowing limited access for unathenticated users

Consider an office with open use PCs in common areas. Staff and customers do not have to log in to these PCs and can use them for limited access to the Internet. From their desks, employees of this office log into PCs which are logged into the office network. The FortiGate unit on the office network uses single sign-on to get user credentials from the network authentication server.

The open use PCs have limited access to the Internet. Employee PCs can access internal resources and have unlimited access to the Internet.

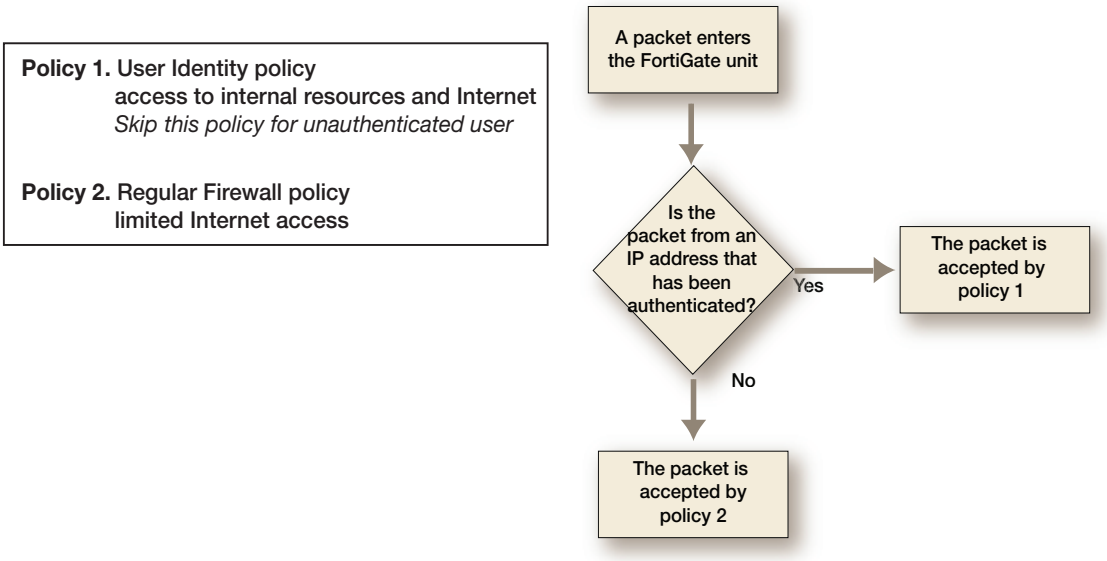
To support these different levels of access you can add a user identity policy to the top of the policy list that allows authenticated users to access internal resources and to have unlimited access to the Internet. In this policy, select *Skip this policy for unauthenticated user*.

Add a normal firewall policy below this policy that allows limited access to the Internet.

Sessions from authenticated PCs will be accepted by the User Identity policy. Sessions from unauthenticated PCs will skip the User Identity policy and be accepted by the normal firewall policy.

Figure 4 shows how the FortiGate unit handles packets received from authenticated and unauthenticated users.

Figure 4: Packet flow for authenticated and unauthenticated users



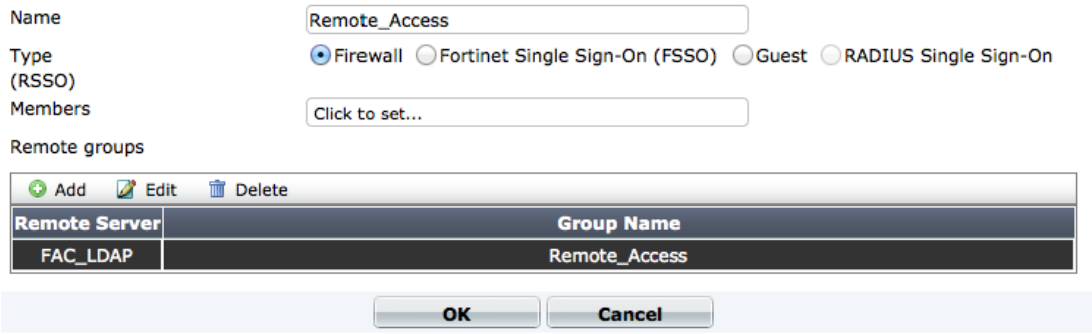
Use case - multiple levels of authentication

As a variation of the above use case, Policy 2 could be a User Identity policy and *Skip this policy for unauthenticated user* would not be selected. Sessions from unauthenticated users that are accepted by Policy2 would now require users to authenticate before traffic can connect through the FortiGate unit. The result is different levels of authentication: Single sign on for some users and firewall authentication for others.

LDAP browser to import users into a user group

You can use the new LDAP browser to add LDAP users to a user group.

Figure 5: The LDAP browser



Dedicated management CPU

FortiGate units in the 2U or High-End categories (models 1000 and above) can now be configured to have a dedicated management CPU. This reserves one CPU core, CPU 0, for running management tasks such as the web GUI, as well as the CLI and related daemons. By having a dedicated management CPU, access to the management GUI and CLI is guaranteed even under when the unit is under a heavy traffic load.

Using a dedicated management CPU may have an impact on the overall performance of the FortiGate unit.

The dedicated management CPU is enabled using the CLI:

```
configure system npu
  set dedicated-management-cpu enable
end
```

Improvements to the Traffic History and Threat History widgets

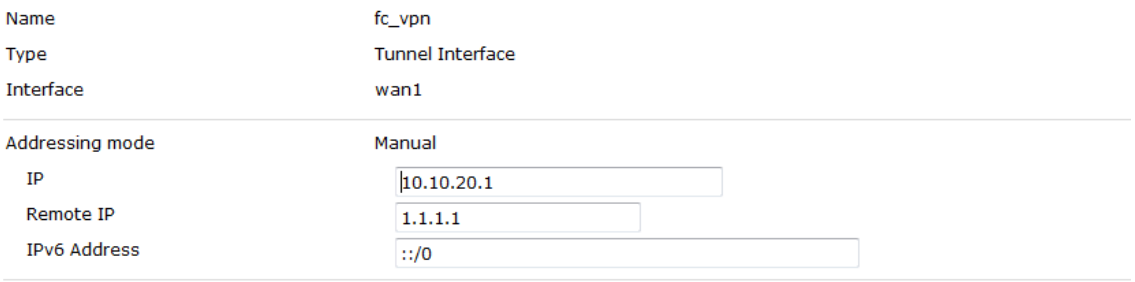
Several changes have been made to the *Traffic History* and *Threat History* widgets:

- The *Show Sessions* and *Show All Incidents* (formerly *Show Threats*) options has been improved to show more information about individual sessions or threats.
- The drilldown page for the *Threat History* widget has been improved by adding new columns and adjusting field formats.
- The *Threat History* widget has replaced the *Reputation Score* monitor used for Client Reputation, which has been removed.

Assigning an IP address to a dynamic IPsec VPN interface

An IP addresses can now be assigned to a dynamic IPsec VPN interface to be used for traffic egressing over the IPsec interface, to avoid traffic being blocked due to an inappropriate address. An IP address is assigned by going to *System* > *Network* > *Interfaces* and editing the interface for the IPsec VPN.

Figure 6: Assigning an IP address to a dynamic IPsec VPN interface



SSL VPN History widget

Login history can now be added to the SSL VPN Portal, which shows a user their past logins. The number of logins shown can be anywhere between 1 and 255 (the default is 5).

The login can be set by going to *VPN* > *SSL* > *Portal,* selecting *Include Login History*, and setting an appropriate *Number of history entries*.

It can also be set using the CLI:

```
config vpn ssl web portal
  edit <portal>
    config widget
      edit <ID>
        set type history
        set display-limit <1-255>
      end
    end
  end
end
```

Port Block Allocation (PBA) for CGN to reduce logs

Port Block Allocation (PBA), a Carrier Grade NAT (CGN) feature, can reduces the number of log messages generated by NAT operations.

PBA can be configured using by going to *Firewall Objects* > *Virtual IPs* > *IP Pools*. It can also be configured using the CLI.

```
config firewall ippool
  edit ippool
    set type port-block-allocation
    set block-size <integer>
    set num-blocks-per-user <integer>
  end
end
```

You configure PBA by creating a private IP address range and assigning multiple port ranges (or blocks) to that IP address range. When a connection is received from the IP range, the source port is translated to a ports in the first range. A log message is written when this happens.

As more connections are received from this IP address range they are assigned to other ports in the first port block. Eventually all of the ports in the block will be used. When a new connection is received, another block of ports is started and a log message is written.

So instead of writing a log message for every NAT event, log messages are only written when a new block of ports is started and again when its used up.

Neighbor cache table for IPv6

A table has now been added to configure IPv6 neighbor cache entries and to save the entries when the FortiGate unit reboots, using the command `config system ipv6-neighbor-cache`.

In the following example, a neighbor cache entry is configured to use the DMZ interface:

```
config system ipv6-neighbor-cache
  edit 1
    set interface dmz
    set ipv6 6666::11
    set mac 00:09:0f:01:02:03
  end
end
```

Improved HA diagnose commands

The new command `diagnose sys ha dump-by` has replaced the command `diagnose sys ha dump`. The new command has the following syntax:

```
diagnose sys ha dump-by {all-xdb | all-vcluster| rcache | all-group |
    memory | debug-zone | vdom | kernel | device | stat| sesync}
```

Each option displays different types of information about the cluster.

The following new HA diagnose commands have also been added:

```
diagnose sys ha sesync-stats
diagnose sys ha extfile-sig
```

Secure disk erasing

All data on the FortiGate boot device and any hard disks installed in a FortiGate unit can now be securely and permanently erased using the `execute erase-disk` command. This command performs a low-level format and also overwrites every block on the device with random data three times.

Anonymize user names in logs

Log messages can now be configured to replace user names with the word ***anonymous***, so that user names are not visible in log messages. This feature can be enabled from the CLI using the following command:

```
config log setting
  set user-anonymize enable
end
```

VLAN interface traffic statistics

A VLAN accounting table has been added to the NP4 driver to poll accounting data from the FortiGate unit in order to monitor traffic statistics from VLAN interfaces. The polling interval is set to 1 second.

Preserving the Class of Service bit

FortiGate units can now preserve the value of the Class of Service (CoS) bit, also called Priority Code Point (PCP), when a packet traverses a VLAN network.

Front panel illustration

An illustrated version of the FortiGate unit's front panel has been added above the list of interfaces, found at *System* > *Network* > *Interfaces*. As with the panel found in the *Unit Operation* widget, interfaces appears green when connected and further details are shown when the mouse pointer hovers over a specific port.

USB entropy token support

Use of a USB entropy token during the boot process is now enabled by default when using a FortiGate in Federal Information Processing Standards-Common Criteria (FIPS-CC) mode. If a FortiGate unit in this mode does not have an USB entropy token inserted, it is unable to complete the boot process will display the following message: `Please insert entropy token to continue boot process`.

Entropy token use can be disabled from the CLI. It can also be enabled on a FortiGate unit in normal mode (by default, entropy tokens are disabled in normal mode).

Syntax

```
config system fips
  set entropy-token {enable | disable}
end
```

The entropy token must be present during boot process when a FortiGate unit is switched to FIPS-CC mode.

Station locate for FortiWiFi units

Station locate allows a FortiWiFi unit to detect all wireless clients whether they are associated or not. A record is kept of MAC address, statistical time interval and RSSI data.

Station locate is enabled using the following CLI command:

```
config wireless-controller wtp-profile
  edit "FAP220B-default"
    config radio-1
      set station-locate enable
      set station-locate-interval 1
    next
    config radio-2
      set station-locate enable
      set station-locate-interval 1
    end
  end
end
```

Switch Controller added to FortiGate models 200D, 240D, 600C, 800C, and 1000C

The Switch Controller, used to managed FortiSwitch units with a FortiGate unit, has been added to the following models: 200D, 240D, 600C, 800C, and 1000C.

Because of this feature, there have been several web-based manager menu changes to these units:

- *WiFi Controller* has changed to *WiFi & Switch Controller*.
- *Managed Access Points* has changed to *Managed Devices* and now contains the *Managed FortiSwitch* option.
- The *Switch Network* menu has been added, which contains the *Virtual Switch* option.

Diagnose command for 5000 series FortiGate units

A new diagnose command, `diagnose test application ipmc_sensord`, is available to view chassis IPMC status from a 5000 series blade installed in a chassis. The command can display:

- Power supply detection
- IPMC sensor status detection
- Comlog enable/disable/info/read/clear
- Smc time set/get
- AMC info
- Microswitch status detection
- HACO info

Because of this change, the following obsolete commands have been removed:

- `get system chassis`
- `get system blades`
- `get chassis status`
- `diag hardware fruinfo`
- `exec bladekvm`

New platforms for FortiGate-VM

FortiGate-VM is now supported for Microsoft Hyper-V and Kernel-based Virtual Machine (KVM).

Supported RFCs

The following RFCs are supported by the new features for FortiOS 5 Patch 5:

Table 1: Supported RFCs

Number	Title
2766	Network Address Translation - Protocol Translation (NAT-PT)
4787	Network Address Translation (NAT) Behavioral Requirements for Unicast UDP
6691	TCP Options and Maximum Segment Size (MSS)

New features in FortiOS 5.0 Patch 4

This chapter provides a brief introduction to the following features that were added to Patch 4 of FortiOS 5.0. See the release notes for a complete list of new features in this release.

FortiSandbox

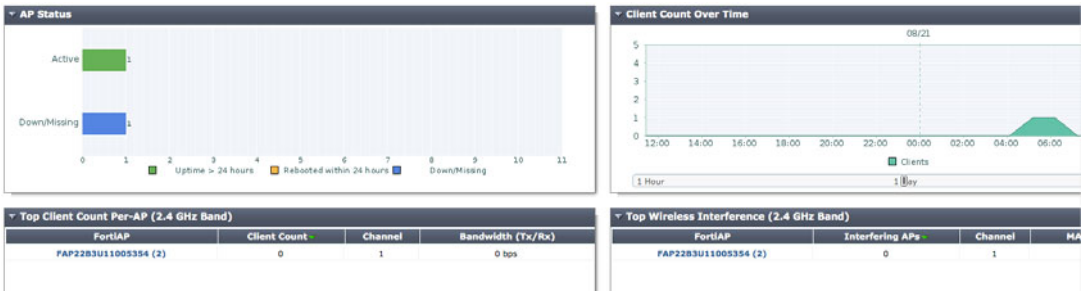
The new FortiSandbox unit can be used with a FortiGate unit for sandboxing suspicious files. Sandboxing can also be done using Cloud Sandbox, which was previously known as FortiGuard Analytics. For more information about this feature, see "FortiSandbox" on page 62.

Wireless Health Dashboard

The Wireless Health Dashboard provides an easy method for determining the health of your network's wireless infrastructure. The dashboard is used to display a variety of widgets, which show information such as AP status, client count over time and login failures.

The dashboard can be found by going to *WiFi Controller* > *Monitor* > *Wireless Health.*

Figure 7: The Wireless Health Dashboard



IPsec VPN

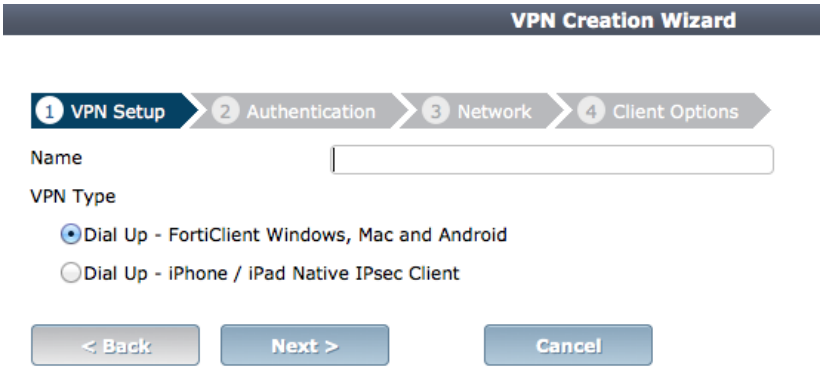
There have been several changes made to how IPsec VPN is configured.

Dial-up IPsec VPN Creation Wizard

A new wizard can be used to create Dial-up IPsec VPNs for FortiClient and Native iOS IPsec clients. The FortiClient configuration can be used for all platforms supported by FortiClient. Find the wizard by going to *VPN* > *IPsec* > *Auto Key (IKE)* and selecting *Create VPN Wizard*.

See http://docs.fortinet.com/sysadmin.html for more information about using the VPN Creation Wizard.

Figure 8: The VPN Creation Wizard



Show or Hide policy-based IPsec VPN

Policy-based IPsec VPN options have been added to the Feature Select options, which controls what features can be viewed and configured through the web-based manager. For more information on this feature, see “Feature Select” on page 168.

By default, policy-based IPsec VPN is hidden from the web-based manager and interface-based VPNs are easier to configure.

Managing FortiAP units

There have been several changes to how FortiAP units are managed by a FortiGate unit.

Units remain online when their WiFi Controller goes offline

FortiAP units can now remain online when their connection to the FortiGate unit's WiFi Controller goes offline. During such an outage, WiFi clients already associated with a bridge mode FortiAP unit continue to remain connected to their SSID and can communicate with other WiFi clients. Access to other network resources; however, is suspended until the FortiGate unit is back online.

The FortiAP unit can also continue to authenticate users if the SSID meets these conditions:

- Traffic Mode is Local bridge with FortiAP's Interface

  In this mode, the FortiAP unit does not send traffic back to the wireless controller.
- Security Mode is either WPA/WPA2-Personal or Open.

  These modes do not require the user database. In WPA/WPA2-Personal authentication, all clients use the same pre-shared key which is known to the FortiAP unit.
- Allow new client association when controller connection is down is enabled.

This field is available only if the other conditions have been met.

Assigning the same profile to multiple FortiAP units

The same profile can now be applied to multiple managed FortiAP units at the same time. To do this, do the following:

1. Go to *WiFi Controller* > *Managed Access Points* > *Managed FortiAPs* to view the AP list.
2. Select all FortiAP units you wish to apply the profile to.
3. Right click on one of the selected FortiAPs and select *Assign Profile*.
4. Choose the profile you wish to apply.

Dynamic VLANs for SSIDs

Dynamic VLANs can now be used to divide a single SSID into several VLANs. In Patch 4, Dynamic VLANs are supported for both tunnel and bridge mode SSIDs.

VLAN assignment is based on the credentials supplied by the user. Dynamic VLANs allow individual users to be assigned different VLANs resulting in different levels of access even though all users are connecting to the same SSID.

The task of assigning users to a specific VLAN is handled by a RADIUS authentication server. When a client attempts to associate to a FortiAP registered with a controller, the FortiAP passes the credentials of the user to the RADIUS server for validation. Once the authentication is successful, the RADIUS server passes certain Internet Engineering Task Force (IETF) attributes to the user. These RADIUS attributes include the VLAN ID that should be assigned to the wireless client.

Dynamic VLANs are configured by doing the following:

1. Go to *User & Device* > *Authentication* > *RADIUS Servers* and create a new RADIUS server.
2. Go to *WiFi Controller* > *WiFi Network* > *SSID* and create a new SSID.
3. Enable Dynamic VLAN in the CLI, using the following command:

```
config wireless-controller vap
  edit <name>
    set dynamic-vlan enable
end
```

4. Go to *WiFi Controller* > *WiFi Network* > *Custom AP* and create a new radio 1 and radio 2 that use the new SSID.
5. Go to *System* > *Network* > *Interfaces* and create two or more VLAN interfaces that have DHCP server enabled.
6. Go to *Policy* > *Policy* > *Policy* and create policies that allow outbound traffic from the new VLANs.
7. Configure a policy on the RADIUS server for each VLAN.

When users scan for available SSIDs, they can connect to the new SSID and be assigned to one of the VLANs based on their credentials.

See http://docs.fortinet.com/supplement.html for some Dynamic VLAN examples.

NAT46 & NAT64

Policies and Virtual IPs for NAT46 and NAT64 can now be configured from the web-based manager. For these options to appear in the web-based manager, this feature must be enabled using Feature Select. For more information, see "Feature Select" on page 168.

To configure NAT64 policies go to *Policy* > *Policy* > *NAT64 Policy*.

To configure NAT46 policies go to *Policy* > *Policy* > *NAT46 Policy*.

Enhancements to Tables

Several enhancements have been made to the tables in the web-based manager to improve access to information.

Policy Table

The following enhancements have been made to the Policy Table:

- The Security Features column has been divided so that each feature has an individual menu, allowing the profile used to be easily visible.
- A pulldown menu will appear when a specific element is selected that displays the other options for the field, as well as showing the *Create New* option.
- The right-click menu has been simplified to show only the options related to the location that was selected. The menu will also change depending on whether a specific element name was selected or if the cell background was selected.

Member Display

The member columns for tables under *Firewall Objects* and *User & Device* have been improved to display members in a grid. When there is a high number of members in a single group, some members will be displayed in the grid, with the hidden members viewed via a dropdown menu.

The number of sub-columns displaying members, the width of sub-columns and the number of lines used to display members are all customizable by right-clicking on the header and selecting *Members Column Option*.

Fortinet Top Bar

In order to ensure that the Fortinet Top Bar appears in all browsers, port 8011 must be allowed in the firewall policy being used.

FortiAnalyzer and FortiManager log encryption

Logs sent to a FortiAnalyzer or FortiManager unit from a FortiGate unit can now be encrypted. Encryption is enabled by going to *Log & Report* > *Log Config* > *Log Settings*.

FortiToken Mobile

There have been several changes made to FortiToken Mobile:

- A QR code image will be attached to FortiToken activation emails.
- Softtoken polling requests have been extended to 5 minutes.
- The range for two factor FortiToken mobile expiry is now 1-168 hours.
- Notifications will be sent when a local user is created.

Load balancing for explicit web proxy forwarding server groups

Explicit web proxy traffic can now be load balanced among multiple forwarding servers in a forwarding server group.

To configure load balancing, add multiple forwarding servers to a forwarding server group and turn on load balancing for the server group. Then add the forwarding server group to a security policy.

The following example adds three forwarding servers to a forwarding server group. Start by creating the forwarding servers:

```
config web-proxy forward-server
  edit fwd-srv-1
    set ip 10.10.10.10
    set port 8080
  next
  edit fwd-srv-2
    set ip 10.10.10.20
    set port 8080
  next
  edit fwd-srv-3
    set ip 10.10.10.30
    set port 8080
  end
```

Then add the forwarding servers to a group:

```
config web-proxy forward-server-group
  edit fwd-srv-grp
    set affinity enable
    set ldb-method weighted
    set group-down-option block
      config server-list
        edit fwd-srv-1
          set weight 10
        next
        edit fwd-srv-2
          set weight 10
        next
        edit fwd-srv-3
          set weight 10
        end
  end
```

Then add the forwarding server group to a web-proxy security policy:

```
config firewall policy
  edit 0
    set srcintf web-proxy
    ...
    set webproxy-forward-server fwd-srv-grp
    ...
  end
```

Server load balancing enhancements

Server load balancing has been enhanced to alert administrators when a server fails and to improve handling of HTTP redirects.

SNMP traps

FortiGate units can now send SNMP traps when the FortiGate unit determines that one of the servers in a server load balance group has gone down. The OID for the trap is *.fgTrapServerLoadBalanceRealServerDown*.

You can use the following CLI command to enable this trap:

```
config system snmp community
  edit 0
    set events load-balance-real-server-down enable
end
```

HTTP redirects

Server load balancing now also supports checking HTTP redirects and setting the maximum number of redirects when 300-level return codes are received.

You can set `http-max-redirects` in the range 0 to 5. The default value is 0 which means do not check redirects, just assume they are available. This is how redirects functioned previously. When you set this option to 1 or more, the FortiGate unit will check up to 5 redirect URLs, until it finds one that is active. Traffic is then re-directed to the first active URL that is found.

Use the following command to check up to 3 redirects:

```
config firewall ldb=monitor
  edit 0
    set set type http
    set port 80
    set http-get "/index.php"
    set http-max-redirects 3
end
```

Additional filters for IPS and Application Control

New filters have been added for IPS and Application Control that will be shown when the *Advanced filter* option is selected on the sensor creation page. The new filters for IPS are Application and Protocol and the new filters for Application Control are Vendor and Protocol.

Blocking IPv6 packets by extension headers

FortiOS can now block IPv6 packets based on the extension headers, using the CLI syntax `config firewall ipv6-eh-filter`.

The following commands are now available:

`set hop-opt {disable | enable}`: Block packets with Hop-by-Hop Options header.

`set dest-opt {disable | enable}`: Block packets with Destination Options header.

`set hdopt-type <integar>`: Block specific Hop-by-Hop and/or Destination Option types (maximum 7 types, each between 0 and 255).

`set routing {disable | enable}`: Block packets with Routing header.

`set routing-type <integar>`: Block specific Routing header types (maximum 7 types, each between 0 and 255).

`set fragment {disable | enable}`: Block packets with Fragment header.

`set auth {disable | enable}`: Block packets with Authentication header.

`set no-next {disable | enable}`: Block packets with No Next header.

Distinguishing between HTTP GET and POST in DLP

Data Leak Prevention (DLP) can now distinguish between HTTP GET and POST protocols, allowing the protocols to be selected independently.

HTTP POST protocol can be examined by both message and file filters, while HTTP GET can only be used for file filters.

RADIUS Accounting

Accounting servers can now be configured in a RADIUS setting. For each RADIUS server, four more accounting servers can be created.

The following example adds an accounting server to a RADIUS server:

```
config user radius
  edit rad159
    set server 172.16.62.159
    set secret asdfasdf
    config accounting-server
      edit 1
        set status enable
        set server 175.18.5.36
        set secret asdfasdf
    end
end
```

H3C Compatibility

FortiOS now has H3C compatibility, allowing 802.1x authentication to be supported with two RADIUS attributes.

The following example enables H3C compatibility:

```
config user radius
  edit rad-jason
    set h3c-compability enable
end
```

Web filter administrative overrides

Administrative web filter overrides can now be configured by going to *Security Profiles* > *Web Filter* > *Web Overrides*. Overrides allow specific users to use an alternate web filter profile, in order to access sites that would normally be blocked.

Configurable idle timeout for console admin login sessions

An idle timeout has been added for FortiGate console sessions (admin sessions connecting to a FortiGate console port or USB port). By default the console timeout is set to 0 and console sessions will never timeout. You can enable a timeout in the range of 15-300 seconds from the CLI. Use the following command to set the timeout to 25 seconds:

```
config sys global
  set admin-console-timeout 25
end
```

Use the following command to disable the timeout.

```
config sys global
  unset admin-console-timeout
end
```

TCP reset

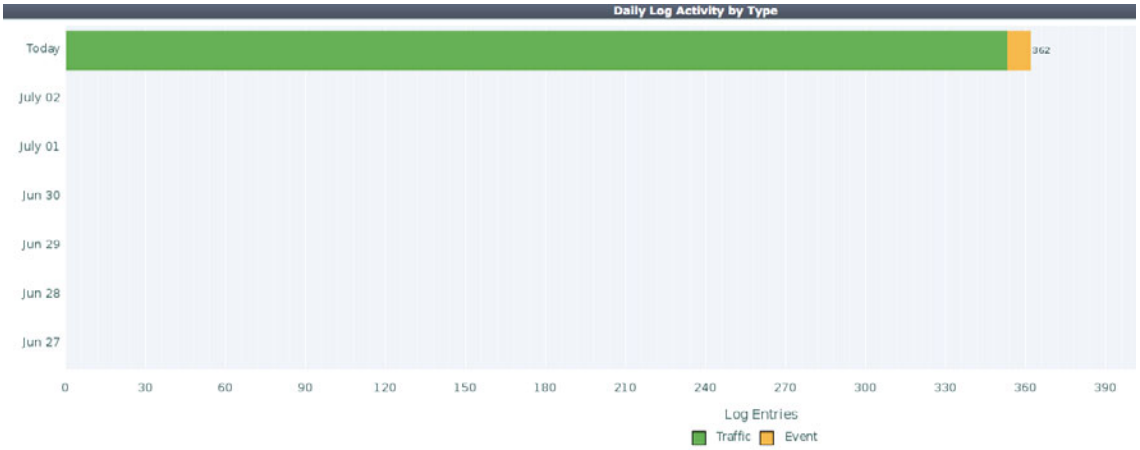
Security policies can now be configured to send a TCP reset when a specific application session times out. The following command is used to enable this function:

```
config firewall policy/policy6
  edit 0
    set timeout-send-rst enable
end
```

Log Volume Monitor

The Log Monitor has been renamed the Log Volume Monitor and has had several visual enhancements made. It can be found at *Log & Report* > *Monitor* > *Logging Volume Monitor*.

Figure 9: The Log Volume Monitor



Invalid Packet log

The Invalid Packet log has been merged with the Local Traffic and Forward Traffic logs. Denied traffic will now appear in either of these logs.

Server limits

The maximum number of virtual and real servers has been increased. The new maximum values vary by FortiGate model and are as follows:

- Desktop FGT: virtual servers, 128 globally; real servers, 4 per entry.
- 1U FGT: virtual servers, 512 globally; real servers, 8 per entry
- 2U FGT: virtual servers, 2048 globally; real servers, 32 per entry.

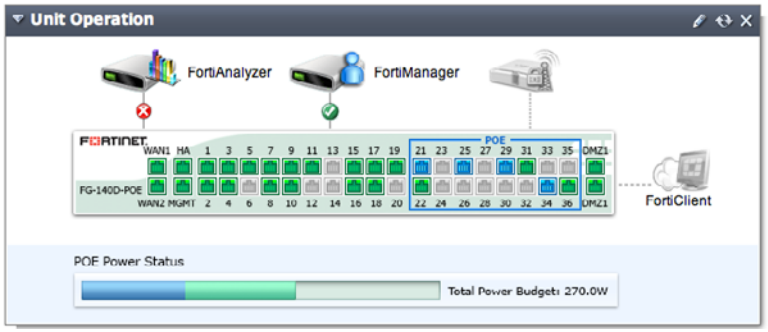
PoE Power Management display

This feature is only available on FortiGate 140D-POE models.

In the *Unit Operation* widget, the *POE Power Status* bar has been added to show the current power output for Power over Ethernet (POE). The bar displays both used power and reserved power.

The port display has also been changed so that the ports that are supplying power appear in blue.

Figure 10: The Unit Operation widget with the POE Power Status bar



Other new features

- Valgrind is now supported in urlfilter daemon, using the following commands:

```
diagnose debug urlfilter valgrind enable
diagnose debug urlfilter valgrind status
diagnose debug urlfilter valgrind memcheck
diagnose debug urlfilter valgrind log
```

- The default post-login banner now displays the time of the last successful and last failed administrator login.

New features in FortiOS 5.0 Patch 3

This chapter provides a brief introduction to the following features that were added to Patch 3 of FortiOS 5.0. See the release notes for a complete list of new features in this release.

Security Features

Features previously known as UTM Security Features are now known as Security Features. For more information about new Security Features in FortiOS 5.0, see “Security Features” on page 62.

Exempting IP addresses from IPS

IPS filters can be configured so that signatures are not applied to traffic from specific IP addresses. For more information about IPS exemptions, see “Exempting IP addresses from IPS” on page 68.

DLP Watermarking Client

The DLP watermarking client is now available for Windows as part of FortiExplorer. For more information about DLP watermarking, see “DLP watermarking” on page 77.

Predefined Device Groups

FortiOS now has Predefined Device Groups for Blackberry Playbook, Router/NAT Device and Windows Tablet. For more information about Predefined Device Groups, see “Device Groups” on page 100.

Client Reputation Configuration

Client Reputation configuration can be found at *Security Profiles* > *Client Reputation.* For more information about Client Reputation, see “Client Reputation” on page 106.

Feature Select

Feature Select replaces the *Display Options on GUI* feature to control which features can be configured and viewed on the web-based manager. For more information on this feature, see “Feature Select” on page 168.

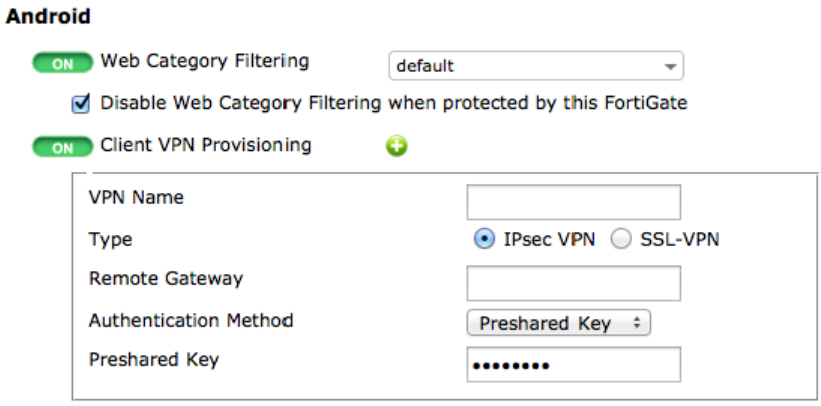
Changes to Endpoint Control

There have been several changes to Endpoint Control.

Endpoint control for Android

FortiOS now supports endpoint control for Android mobile devices. Endpoint profiles that include Android devices can be configured at *User & Device* > *Endpoint Protection* > *FortiClient Profiles.*

Figure 11: Endpoint control for Android



Assigning endpoint profiles to specific users and user groups

Endpoint profiles can now be assigned to specific users and user groups that have been defined on the FortiGate. This can be done from the CLI, using the following command:

```
config endpoint-control profile
  edit <profile-name>
    set users <user-name>
    set <user-groups> <user-group-name>
end
```

Endpoint profile portal pages

Custom endpoint profile portal pages can be configured. There are five different portals that can be used, depending on the operating system of the endpoint device. The five portals are: Android, Mac, iOS, Windows and other. To access the portal pages, go to *System* > *Config* > *Replacement Messages* and select *Extended View*.

Managing FortiAP units

There have been several changes to how FortiAP units are managed by a FortiGate unit.

Firmware Auto-detection

A FortiGate unit now auto-detects what the best firmware version is for the FortiAP units that it manages. If the FortiAP unit is not running the recommended firmware version you can download and install in from the FortiGate web-based manager.

Wireless Device Locating Service

A FortiAP unit can be configured to report all wireless devices that it locates, even if the device does not connect, or is unable to connect, to the FortiAP.

Locating service is enabled from the CLI, using the following command:

```
config wireless-controller wtp-profile
  edit "FAP220B-default"
    set ap-country JP
    config radio-1
      set station-locate enable
    end
    config radio-2
      set station-locate enable
    end
end
```

After this configuration is complete, the list of devices can be found using the following command:

```
diagnose wireless-controller wlac -c sta-locate
```

The command displays a list of currently located wireless devices. The list includes the MAC address of each device as well as wireless-related information about the device.

More Wireless Controller MIB Support

More fields related to wireless controller functionality has been added to the FortiGate MIB. Additions include the following:

- Asynchronous notifications from SNMP agent, including fgTrapWcApUp and fgTrapWcApDown.
- Objects defined for controller level information, for example: controller name and location, WTP capacity and count and station capacity and count.
- A set of objects that display a WLAN interface, for example: assigned SSID and security method.
- An object identifier for a list of tables pertaining to WTPs.
- A set of objects that display a custom WTP profile, for example: profile name, platform type, DTLS policy and country code.
- A set of objects that display a radio in a custom WTP profile, for example: radio mode, band and channel settings, power level and VAP configurations.
- A set of objects that display the configuration of a WTP, for example: WTP ID, name and assigned custom profile. If no custom profile is assigned, then a list of objects that supplement the automatic profile are defined.
- A set of objects that display wireless session information, for example: IP/MAC address, connection state, up time, profile name, WTP HW/SW information, WTP session statistics, CPU load and memory capacity and usage.
- A set of objects that display wireless session radio information, for example: radio mode, operating country code, operating channel, operating power level and client count.
- A set of objects that display a virtual access point (a WLAN allocated on a WTP radio), for example: client count and RX/TX byte counts.

A set of objects that display a wireless station, for example: WTP and radio it connects to, IP/MAC address, VCI/host information, signal/noise level, TX/RX bandwidth, channel, security type and on-line status.

Normal or Remote WTP mode parameter

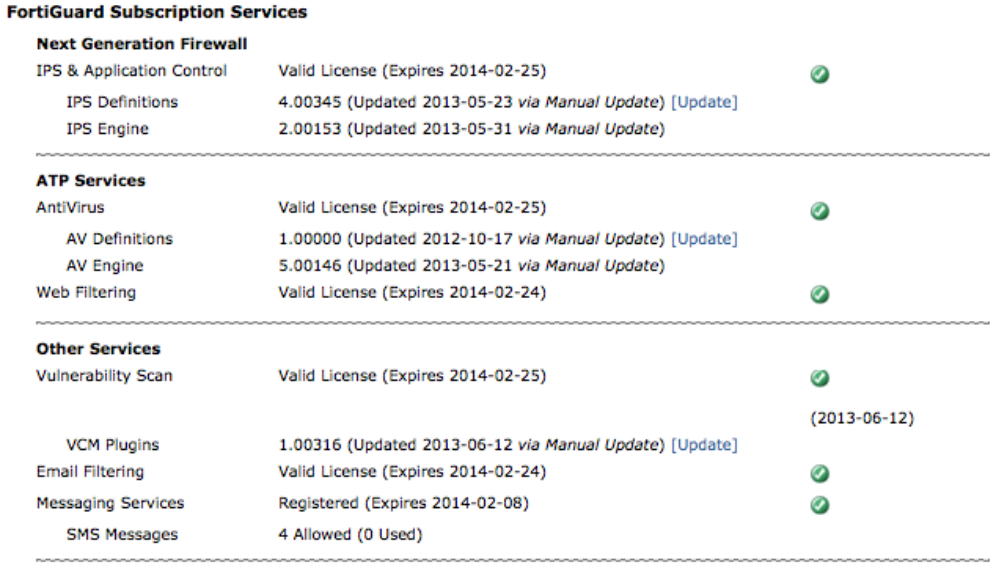
A new WTP mode parameter has been added in which FortiAP units are classified as either normal or remote. A FortiAP unit in normal mode uses SSID in tunneled mode while remote WTP mode uses only local bridge SSIDs.

This new mode has changed the maximum number of FortiAP units which can be managed by a FortiGate unit, with one value for the maximum number of normal FortiAPs and another for the maximum number of remote FortiAPs. For more information, see the Maximum Values Table for FortiOS 5.0.

FortiGuard Subscription Services

The FortiGuard Subscription Services have been reorganized into three categories: Next Generation Firewall, ATP Services and Other Services.

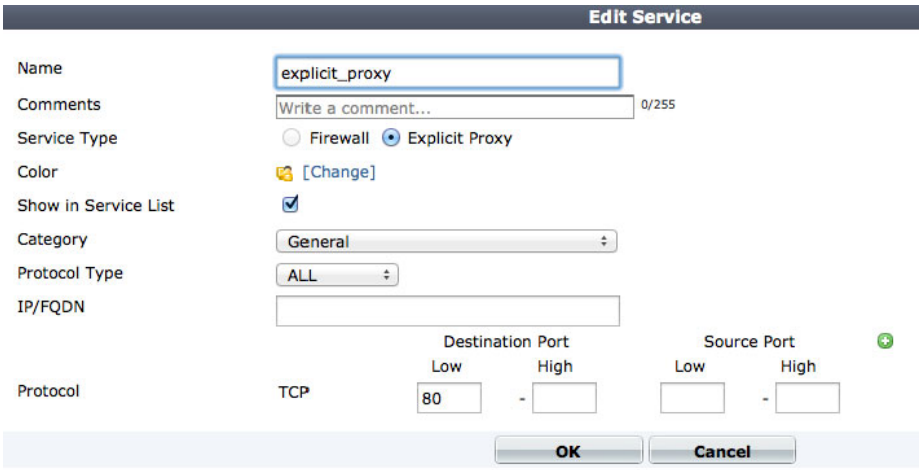
Figure 12: The FortiGuard Subscription Services



Adding Explicit Web Proxy services

Explicit proxy services can now be added and edited by going to *Firewall Objects* > *Service* > *Services* > *Create New* > *Custom Service* and selecting *Explicit Proxy*. Explicit web proxy services are used in security policies that control access to the explicit web proxy.

Figure 13: Editing an Explicit Web Proxy Service

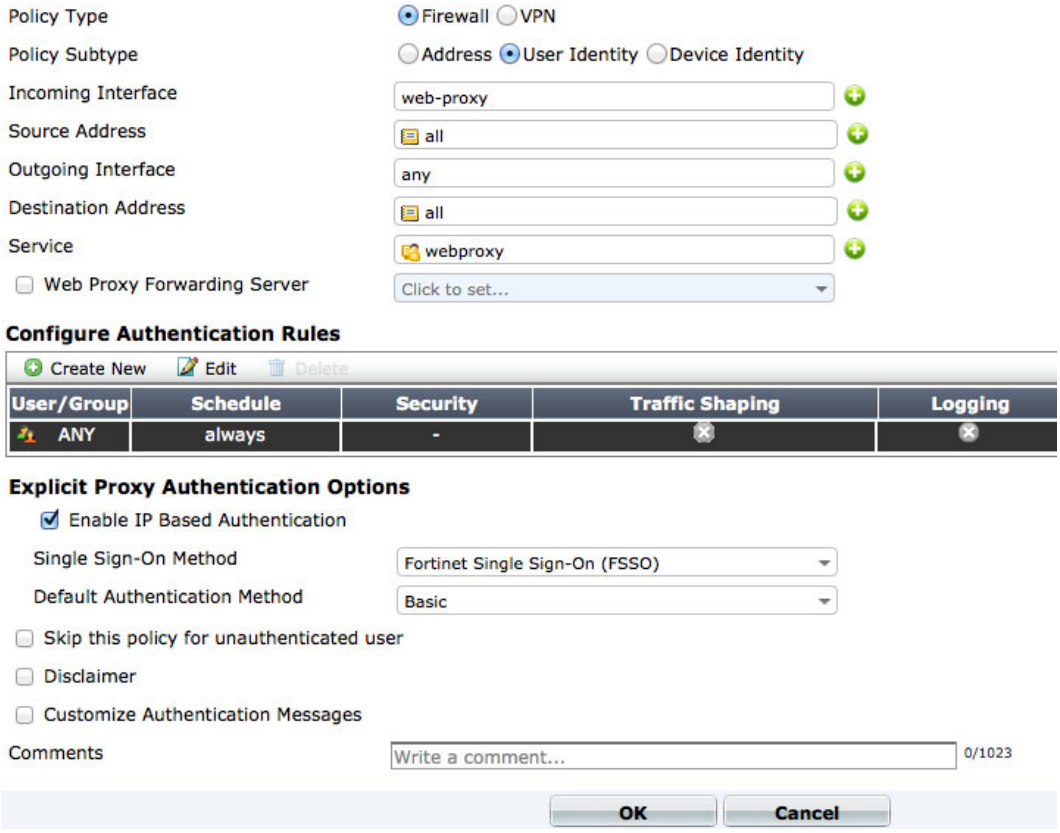


SSO Authentication failover for the Explicit Web Proxy

SSO authentication failover for the Explicit Web Proxy is now available, allowing two authentication methods to be configured. If the Single Sing-On Method fails, the FortiGate unit will use the *Default Authentication Method*.

To configure failover, the explicit web proxy must first be enabled.

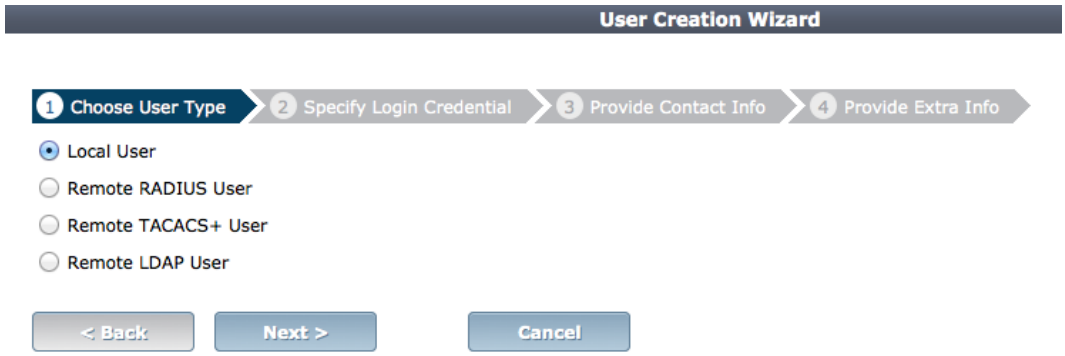
Figure 14: Configuring SSO authentication failover for the explicit web proxy



User Creation Wizard

The User Creation Wizard is used to create new users through a four step process. The four steps will vary depending on which type of user is being created (for example, when creating an LDAP user, step 3 requires choosing an LDAP filter).

Figure 15: The User Creation Wizard



The User Creation Wizard can be found at *User & Device* > *User* > *User Definition*.

FortiClient Registration

The FortiClient registration process has changed so that the initial confirmation message sent from FortiClient will be ignored by the FortiGate unit and applied only at the end of the registration process, to avoid the registration being rejected.

DSS and ECDSA Certificates for FortiGate SSL-related features

FortiOS now supports DSS and ECDSA certificates for the following features: HTTPS/SSL deep scanning, HTTPS/SSL server load balancing, HTTPS/SSL offloading and HTTPS over the explicit web proxy.

LDAP Servers

A Distinguished Name field and query button have been added to the LDAP Server creation page.

User Monitor

FSSO Logons are now shown in the user monitor, found at *User & Device* > *Monitor* > *Firewall*. In order for FSSO Logons to appear, *Show all FSSO Logons* must be enabled.

Web Filter Profiles

URL filters, used for website filtering, are now created as part of a Web Filter Profile. This can be done by going to *Security Profiles* > *Web Filter* > *Profiles* and selecting *Enable Web Site Filter*. A filter can then be enabled for all URLs you wish to block.

CAPWAP Administrative Access

CAPWAP Administrative Access can now be configured for all interfaces except Virtual Access Points (VAPs). CAPWAP must be used on any interface used to managed a FortiAP unit.

IPS Algorithms

There is a new algorithms for IPS, “super” mode, that improves performance for FortiGate units with more than 4GB of memory. Improvements have also been made for “low” mode, which is more efficient for FortiGate units with low memory.

The algorithm used for IPS can be changed from the CLI, using the following command:

```
config ips global
   set algorithm {engine-pick | high | low | super}
```

NAC-Quarantine Traffic Logs

Antivirus and DLP NAC-quarantine traffic logs now show whether the IP, user or interface has been banned. In the case of a virus, the name of the virus and the file in which the virus was found are also included.

New System Report Charts

The following charts have been added to the daily FortiGate System Report, based on data collected by event logs:

- VPN Usage
- Client Reputation Summary

Memory Logging

Memory logging is available on all FortiGate models. Logging can be enabled by going to *Log & Report* > *Log Config* > *Log Settings* and enabling *Disk*.

Logging to flash is also available for the FortiGate-60D and FortiWiFi-60D.

URL-based Web Proxy Forwarding

In order to configure URL-based web proxy forwarding, *WAN Opt. & Cache* must be enabled using Feature Setting. For more information, see “Feature Select” on page 168.

FortiOS now supports URL-based web proxy forwarded, which is required for explicit proxy installations using Threat Management Gateway or Blue Coat.

URL-based web proxy forwarding can be configured by going to *WAN Opt. & Cache* > *Cache* > *URL Match List*.

Changes to Routing

There following changes have occurred for FortiOS Routing:

- The OSPF summary address limit has decreased to 25 from 10.
- More routing community lists can be configured (limits vary by FortiGate model).

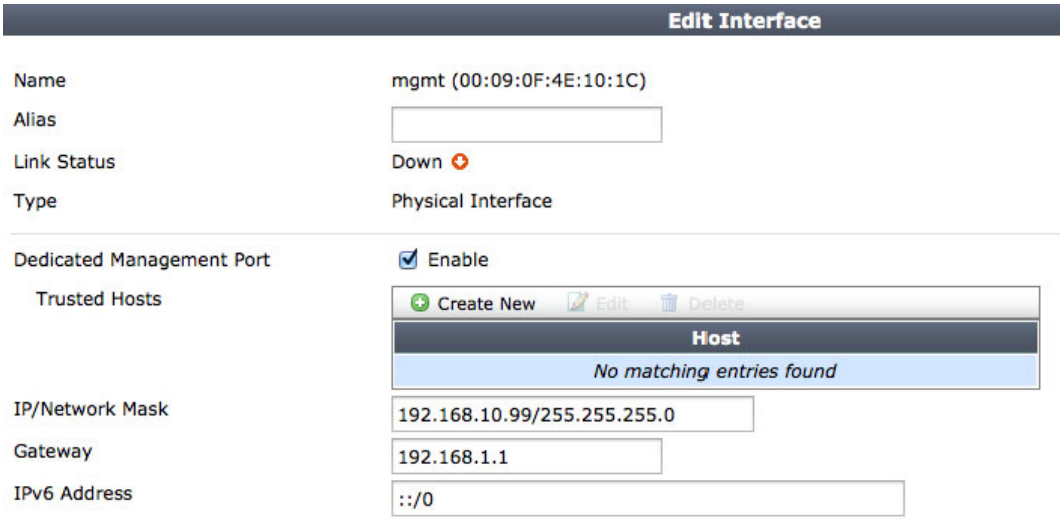
RADIUS Support for Dynamic VLANs

RADIUS authentication can be used to dynamically route authenticated user traffic to a VLAN. The name of this VLAN is then added to the user's RADIUS record.

Dedicated Management Port

The Management (MGMT) port can now be set as Dedicated to Management, in which case no firewall traffic will be allowed through this port.

Figure 16:MGMT port set to Dedicated to Management



URL Filtering

URL filtering has changed to allow certificate-based URL filtering for HTTPS traffic, which is used when deep-scan is disabled.

Certificate-based filtering extracts the hostname from the TLS handshake. If a valid hostname is found, it is used for the local or FortiGuard category query. If no hostname is found, HTTPS server CN web filtering will be used instead.

URL Source Tracking

URL source tracking has been added to transparent proxy and SSL deep-inspection proxy. There are three current URL source values: HTTP host head, subject CN in the certificate and server name field in the TLS handshake.

IPv6 Denial of Service Policies

Denial of Service (DoS) policies can now be configured by going to *Policy* > *Policy* > *IPv6 Dos Policy*.

Support for NAT46, VIP64 and VIP46

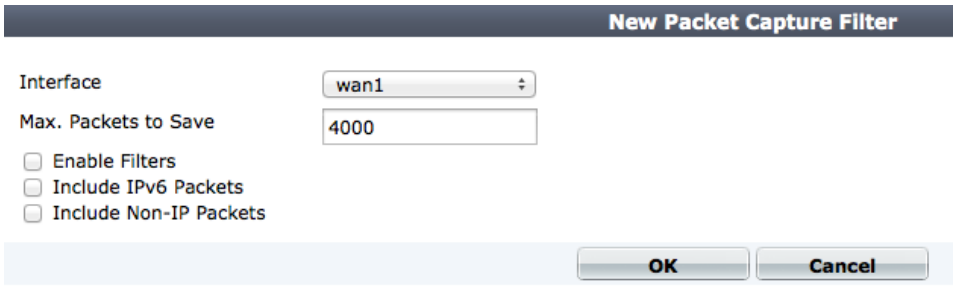
Security policies are now supported for NAT46, VIP64 and VIP46. They can be configured from the CLI, using the following commands:

```
config firewall policy46
config firewall vip64
config firewall vip46
```

Packet Capture Filters

Packet capture filters can be configured by going to *System* > *Network* > *Packet Capture*.

Figure 17: Configuring a packet capture filter



Configure hosts in an SNMP v1/2c community to send queries or receive traps

When you add a host to an SNMP v1/2c community you can now decide whether the FortiGate unit will accept queries from the host or whether the FortiGate unit will send traps to the host. You can also configure the host for both traps and queries.

Use the following command to add two hosts to an SNMP community:

- An IPv4 host that can send queries to the FortiGate unit
- An IPv6 host that the FortiGate unit will send traps to

```
config system snmp community
  config hosts
    edit 1
      set interface port1
      set ip 172.20.120.1
      set host-type query
    end
  config hosts6
    edit 1
      set interface port6
      set ip 2001:db8:0:2::30
      set host-type trap
    end
```

You can add up to 16 IPv4 hosts and up to 16 IPv6 hosts.

IP in IP tunneling support (RFC 1853)

FortiOS 5.0 MR3 supports RFC 1853 IP in IP Tunneling to provide for differential forwarding to packets. This tunneling mechanism is supported as an interface type and the FortiGate unit does not inspect the traffic in an IP in IP tunnel

To configure IP in IP tunneling:

```
config system ipip-tunnel
  edit tun0
    set interface <interface_name>
    set local-gw <local-gw-ip>
    set remote-gw <remote-gw-ip>
  end
end
```

GTP-u acceleration on FortiGate units with SP3 processors

FortiGate units with SP3 processors can offload GTP-u packet processing to their SP3 processor. The SP3 processor supports:

- GTP-u sanity packet check
- GTP-u rate limiting per gtp profile
- Encapsulated IP traffic filtering

New features in FortiOS 5.0 Patch 2

This chapter provides a brief introduction to the following features that were added to Patch 2 of FortiOS 5.0. See the release notes for a complete list of new features in this release.

Endpoint Profile Changes

A number of changes have been made to enhance Endpoint Profile functionality.

Client Reputation Changes

A number of changes have been made to enhance Client Reputation functionality. For information about how to configure and use Client Reputation, see “Client Reputation” on page 106.

Changes to logging in security policies

Instead of enabling or disabling traffic logging in security policies three Logging Options are now available:

- *No Log*, do not record log messages about traffic accepted by this security policy
- *Log UTM Events*, record traffic log messages when a UTM event occurs (such as when a virus is found by antivirus, a web page is blocked by web filtering, or the application responsible for a session is identified by application control).
- *Log all Sessions*, record traffic log messages for all sessions. For all sessions, a single traffic log message is recorded when the session ends. If you select this option, you can choose to record a traffic log message when a session starts as well. You can also choose to capture packets.

Enabling logging in a security policy can affect FortiGate performance because of the extra system resources required to record log messages. The performance hit can be reduced by selecting *Log UTM Events,* since fewer log messages will be recorded.

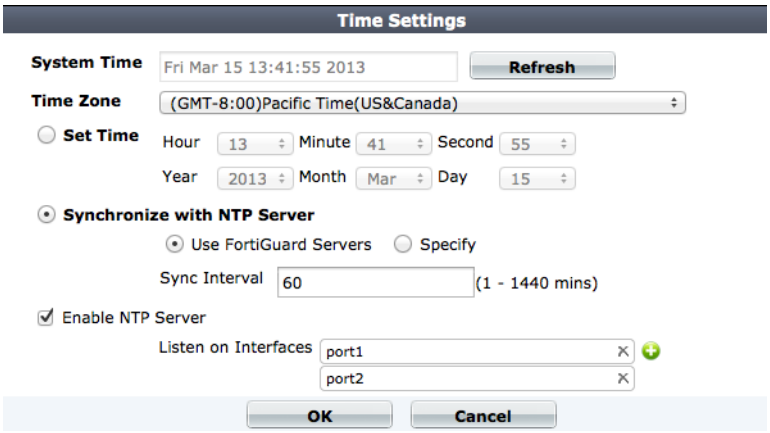
You can also enter the following command to write a log message when a session starts:

```
config firewall policy
  edit <policy-index>
    set logtraffic-start
  end
```

Configuring the FortiGate unit to be an NTP Server

When you configure system time from the System Information dashboard widget, you can configure the FortiGate unit to be an NTP server. As part of the NTP server configuration, you can select one or more interfaces on which to listen for NTP requests.

Figure 18: System time configuration: NTP server



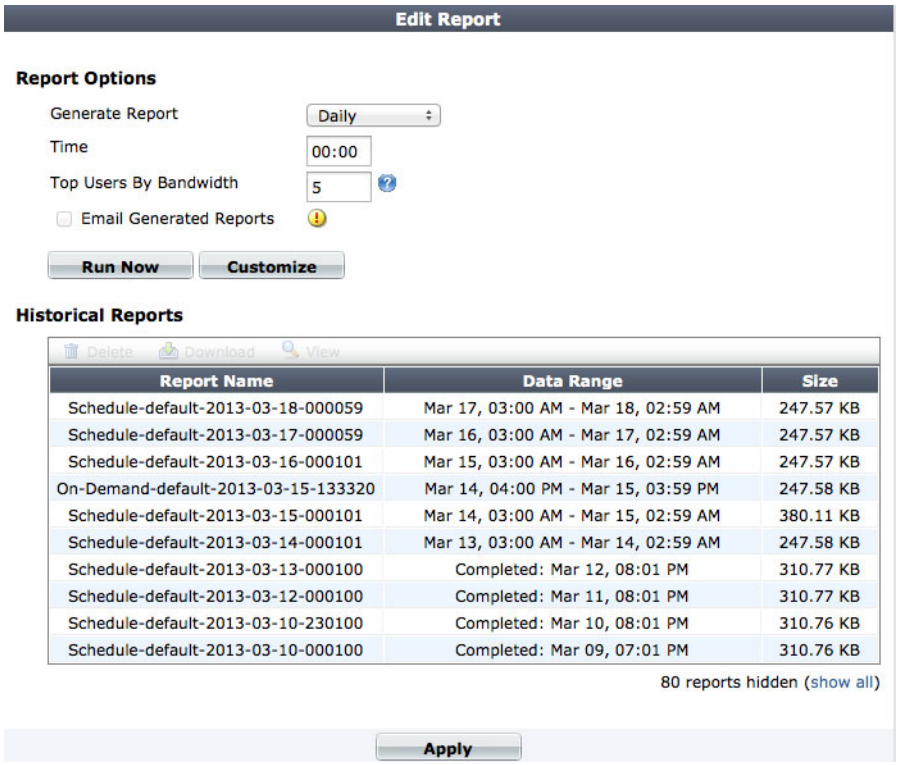
Customizing and viewing the local FortiGate UTM Security Analysis Report

In order for your FortiGate unit to create a Security Analysis Report, disk logging must be enabled. To enable disk logging, go to *Log & Report* > *Log Config* > *Log Settings* and under *Logging and Archiving* select *Disk* and *Enable Local Reports*.

You can go to *Log & Report* > *Report* > *Local* to view Local Reports created by the FortiGate unit. Local reports are saved as PDF files that you can view and download at any time.

By default, Local reports are produced every day. You customize how the FortiGate unit to produce reports daily, weekly, or on demand and you can set the day and time when the report is generated. You can control how many users appear in the Top Users by bandwidth summary part of the report. Each user gets a separate summary page. You can also configure the FortiGate unit to email the report to multiple email recipients.

Figure 19: Customizing the FortiGate report



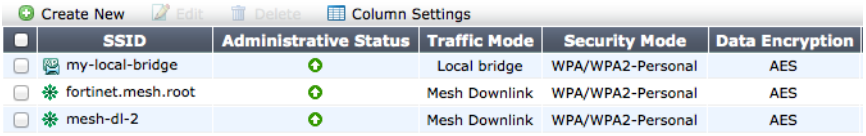
You can also select *Run Now* to run a report at any time. The report is created using current data.

You can select *Customize* to change the report layout. You can customize a report to add headings and text, divide a report into sections, add images, and add, remove, and rearrange the individual report charts.

Wireless changes: Custom mesh downlink SSIDs and new identifier for local bridge SSIDs

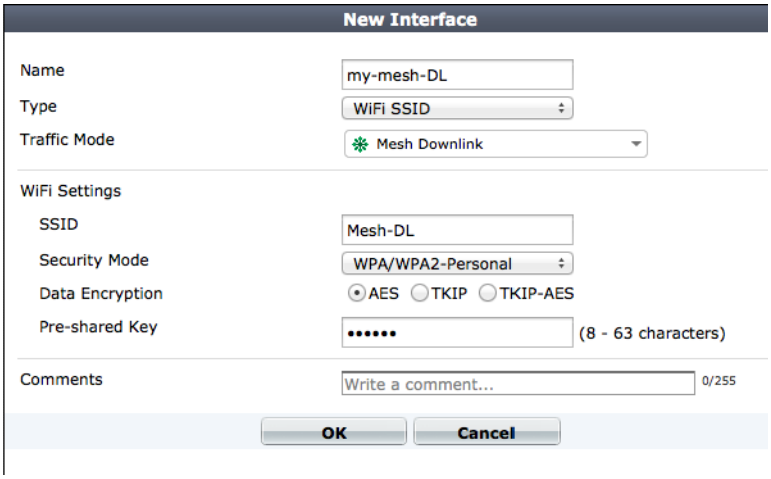
You can go to *WiFi Controller* > *WiFi Network* > *SSID* and select *Create New* to add additional custom mesh downlink SSIDs.

Figure 20:SSID list showing a local-bridge SSID and two mesh downlink SSIDs



Configure a mesh downlink SSID by selecting *Create New,* setting the *Traffic Mode* to *Mesh Downlink* and entering an SSID.

Figure 21: Configuring a custom mesh downlink



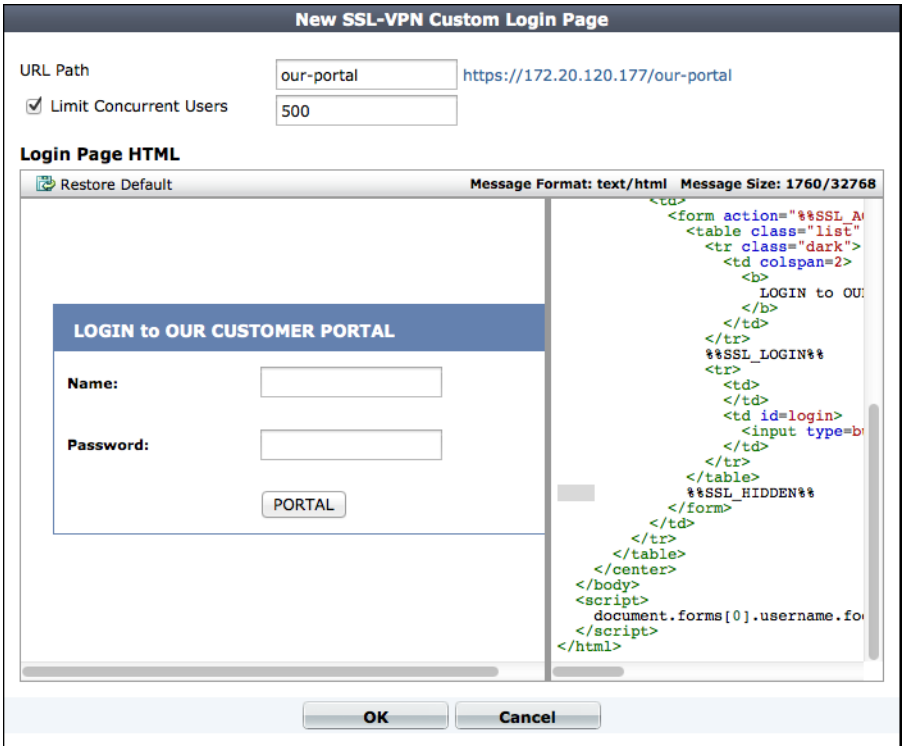
SSL-VPN Realm Support (multiple custom SSL VPN logins)

In order to create a custom login page using the web-based manager, this feature must be enabled using Feature Select. For more information, see “Feature Select” on page 168.

You can go to *VPN* > *SSL* > *Custom Login* and create custom login pages for your SSL VPN users. You can use this feature to customize the SSL VPN login page for your users and also to create multiple SSL VPN logins for different user groups.

You configure a custom SSL VPN login by going to *VPN* > *SSL* > *Custom Login* and selecting *Create New*. Users access different portals depending on the URL they enter. The first option in the custom login page is to enter the path of the custom URL. This path is appended to the address of the FortiGate unit interface that SSL VPN users connect to. The actual path for the custom login page appears beside the URL path field. You can also limit the number of users that can access the custom login at any one time. Finally you can use HTML code to customize the appearance of the login page.

Figure 22: Custom SSL VPN login



After adding the custom login, you must associate it with the users that will access the custom login. Do this by going to *Policy* > *Policy* > *Policy* and creating an SSL VPN policy. Add an *Authentication Rule* to the policy and select the users and user groups who should access the custom login page. Select *Custom Login* and select the custom login page that you created.

Figure 23: Associating a custom SSL VPN login with a user group

Automatically add devices found by device identification to the vulnerability scanner configuration

When you go to *System* > *Network* > *Interfaces* to configure an interface to detect and identify devices you can also select *Add New Devices to Vulnerability Scan List*. As devices are found, they are added to the Asset Definitions list of the Vulnerability scanner. You can choose to run a scan of all of the devices on the list or of selected items, including devices found using FortiGate device identification.

The SIP ALG can receive SIP traffic on multiple TCP and UDP ports

You also configure the SIP ALG to listen in two different TCP ports and two different UDP ports for SIP sessions. For example, if you receive SIP TCP traffic on port 5060 and 5064 and UDP traffic on ports 5061 and 5065, you can enter the following command to receive the SIP traffic on all of these ports:

```
config system settings
  set sip-tcp-port 5060 5064
  set sip-udp-port 5061 5065
end
```

IPv6 PIM sparse mode multicast routing

FortiOS supports PIM sparse mode multicast routing for IPv6 multicast (multicast6) traffic and is compliant with RFC 4601: Protocol Independent Multicast - Sparse Mode (PIM-SM). You can use the following command to configure IPv6 PIM sparse multicast routing.

```
config router multicast6
  set multicast-routing {enable | disable}
    config interface
      edit <interface-name>
        set hello-interval <1-65535 seconds>
        set hello-holdtime <1-65535 seconds>
    end
    config pim-sm-global
      config rp-address
        edit <index>
          set ipv6-address <ipv6-address>
    end
```

The following diagnose commands for IPv6 PIM sparse mode are also available:

```
diagnose ipv6 multicast status
diagnose ipv6 multicast vif
diagnose ipv6 multicast mroute
```

Wireless RADIUS-Based MAC Authentication

Wireless clients can be supplementally authenticated by MAC address. A RADIUS server stores the allowed MAC address for each client and the wireless controller checks the MAC address independently of other authentication methods.

MAC-based authentication must be configured in the CLI. In the following example, MAC-based authentication is added to an existing access point *vap1* to use a RADIUS server at 192.168.1.95:

```
config wireless-controller vap
  edit vap1
    set radius-mac-auth enable
    set radius-mac-auth-server 192.168.1.95
end
```

Security Features

Features previously known as UTM Security Features are now known as Security Features.

In order to create new profiles for the Security Features, Multiple Security Profiles must be enabled using Feature Select. For more information, see “Feature Select” on page 168.

New Security Features in FortiOS 5.0 include:

- FortiSandbox
- Botnet and phishing protection
- Windows file sharing (CIFS) flow-based antivirus scanning
- Advanced Application Control and IPS sensor creation
- Custom Application Control signatures and IPS signatures
- Flow-based inspection improvements
- Configuring SSL inspection for flow-based and proxy protection
- Explicit web Proxy Extensions – SSL inspection, IPS, Application Control, and flow-based antivirus, web filtering and DLP
- Replacement messages for flow-based web filtering of HTTPS traffic
- DNS web filtering
- FortiGuard Web Filter quotas can be set based on traffic volume
- Customizing the authentication replacement message for a FortiGuard web filter category
- YouTube Education Filter implemented in Web Filtering Profiles
- IPS hardware acceleration
- New SIP ALG features
- DLP watermarking
- SSH inspection
- Optimizing SSL encryption/decryption performance

FortiSandbox

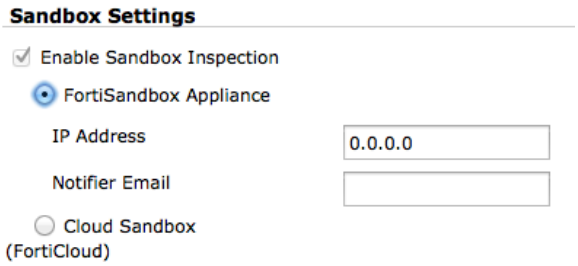
The new FortiSandbox unit is used for automated sample tracking, or sandboxing, for files from a FortiGate unit. This allows suspicious files to be sent to be inspected without risking network security. If the file exhibits risky behavior, or is found to contain a virus, a new virus signature is created and added to the FortiGuard antivirus signature database.

Cloud Sandbox, formerly known as FortiGuard Analytics, can also be used for sandboxing if you have an active FortiCloud subscription.

Configuration

FortiSandbox is configured by going to *System* > *Config* > *FortiSandbox*. After enabling FortiSandbox, select either: *FortiSandbox Appliance* or *Cloud Sandbox (FortiCloud)*.

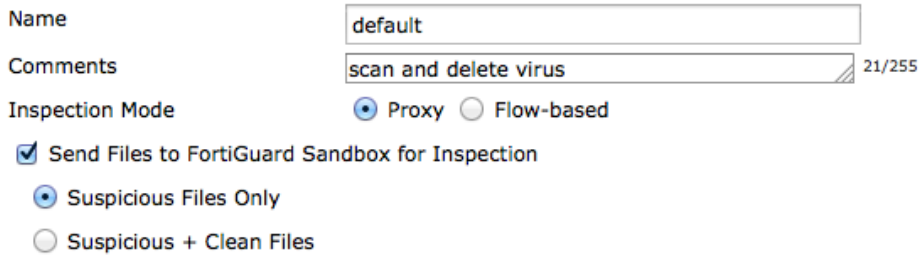
Figure 24: FortiSandbox Configuration



Sending files to FortiSandbox

An anti-virus profile can be set up to send files to FortiSandbox. To do this, edit the profile being used and enable *Send Files to FortiSandbox for Inspection*.

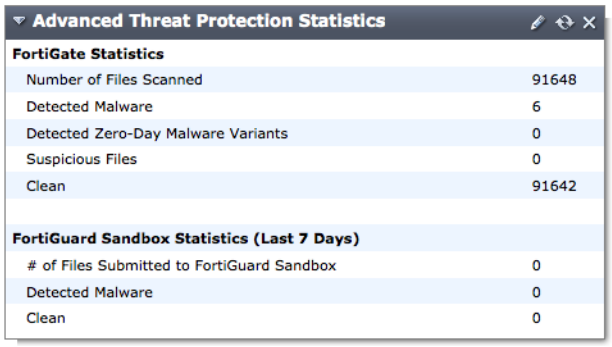
Figure 25: An anti-virus profile using FortiSandbox



Tracking submitted files

The *Advanced Threat Protection Statistics* widget shows the number of files that have been submitted to FortiSandbox and the inspection results.

Figure 26: The Advanced Threat Protection Statistics widget

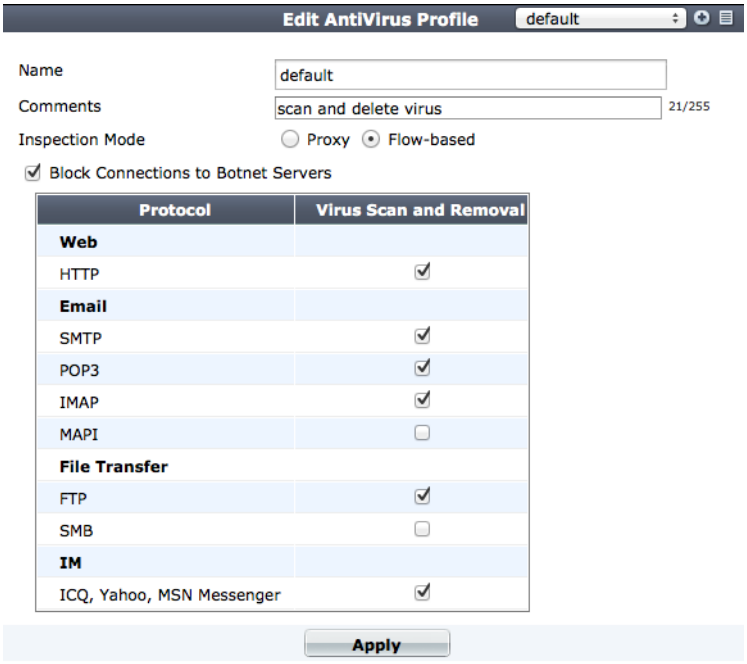


Botnet and phishing protection

In a proxy or flow-based antivirus profile, you can configure the FortiGate unit to detect and block botnet server connection attempts. This feature also blocks attempted access to phishing URLs. The antivirus database is constantly updated with the addresses of known command and control (C&C) sites that Botnet clients attempt to connect to as well as phishing URLs.

To enable Botnet and phishing protection in either a proxy or flow-based antivirus profile, select *Block Connections to Botnet Servers*.

Figure 27: Adding Botnet and phishing protection to a flow-based antivirus profile

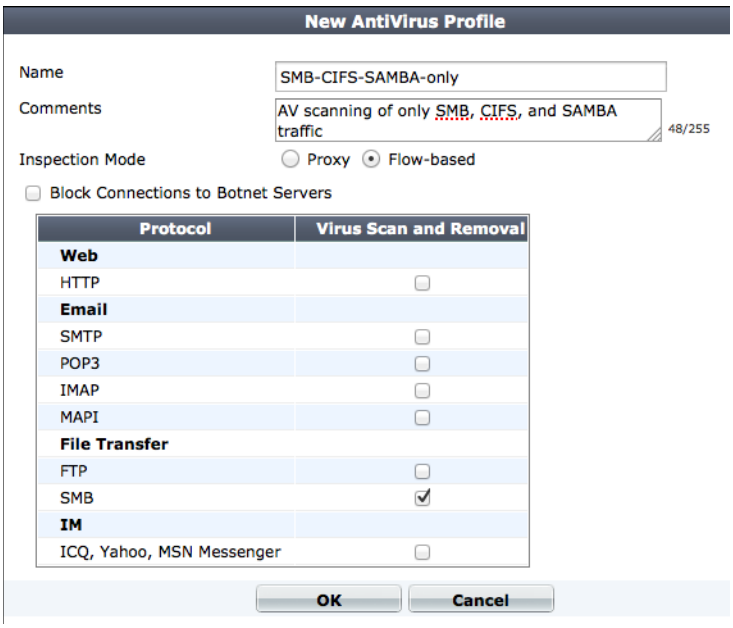


Windows file sharing (CIFS) flow-based antivirus scanning

FortiOS 5.0 now supports virus scanning of Windows file sharing traffic. This includes CIFS, SMB and SAMBA traffic. This feature is applied by enabling SMB scanning in an antivirus profile and then adding this profile to a security policy that accepts CIFS traffic. CIFS virus scanning is available only through flow-based antivirus scanning.

FortiOS 5.0 flow-based virus scanning can detect the same number of viruses in CIFS/SMB/SAMBA traffic as it can for all supported content protocols.

Figure 28: Configuring CIFS/SMB/SAMBA virus scanning



Use the following command to enable CIFS/SMB/SAMBA virus scanning in an antivirus profile:

```
config antivirus profile
  edit smb-profile
    config smb
      set options scan
      set avdb flow-based
    end
```

Then add this antivirus profile to a security policy that accepts the traffic to be virus scanned. In the security policy the service can be set to ANY, SAMBA, or SMB.

```
config firewall policy
  edit 0
    set service ANY
    ...
    set utm-status enable
    set av-profile smb-profile
  end
```

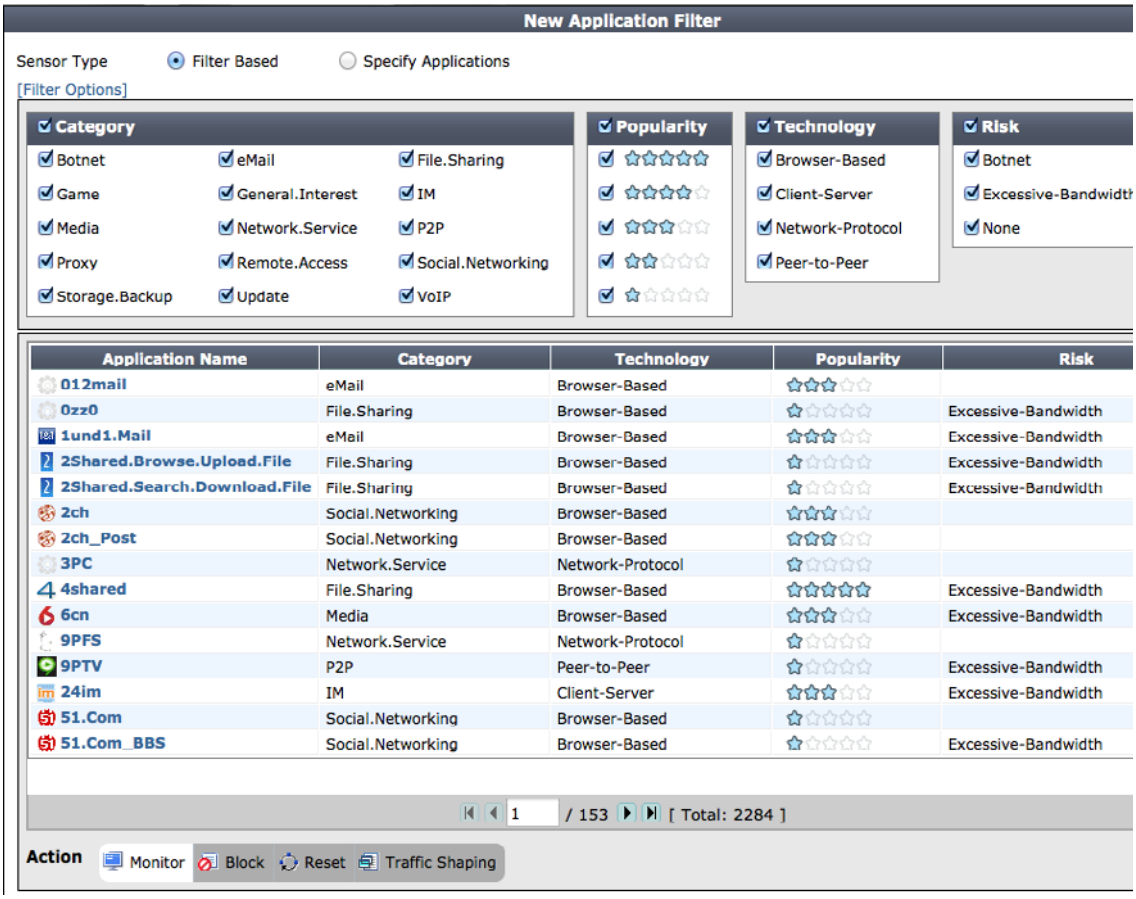
Note the following about CFIS/SMB/SAMBA virus scanning:

- Some newer version of SAMBA clients and SMB2 can spread one file across multiple sessions, preventing some viruses from being detected.
- Enabling CIFS/SMB/SAMBA virus scanning can affect FortiGate performance.
- SMB2 is a new version of SMB that was first partially implemented in Windows Vista. Currently SMB2 is supported by Windows Vista or later, partly supported by Samba 3.5 and fully support by Samba 3.6.
- The latest version of SMB2.2 will be introduced with Windows 8.
- Most clients still use SMB as default setting.

Advanced Application Control and IPS sensor creation

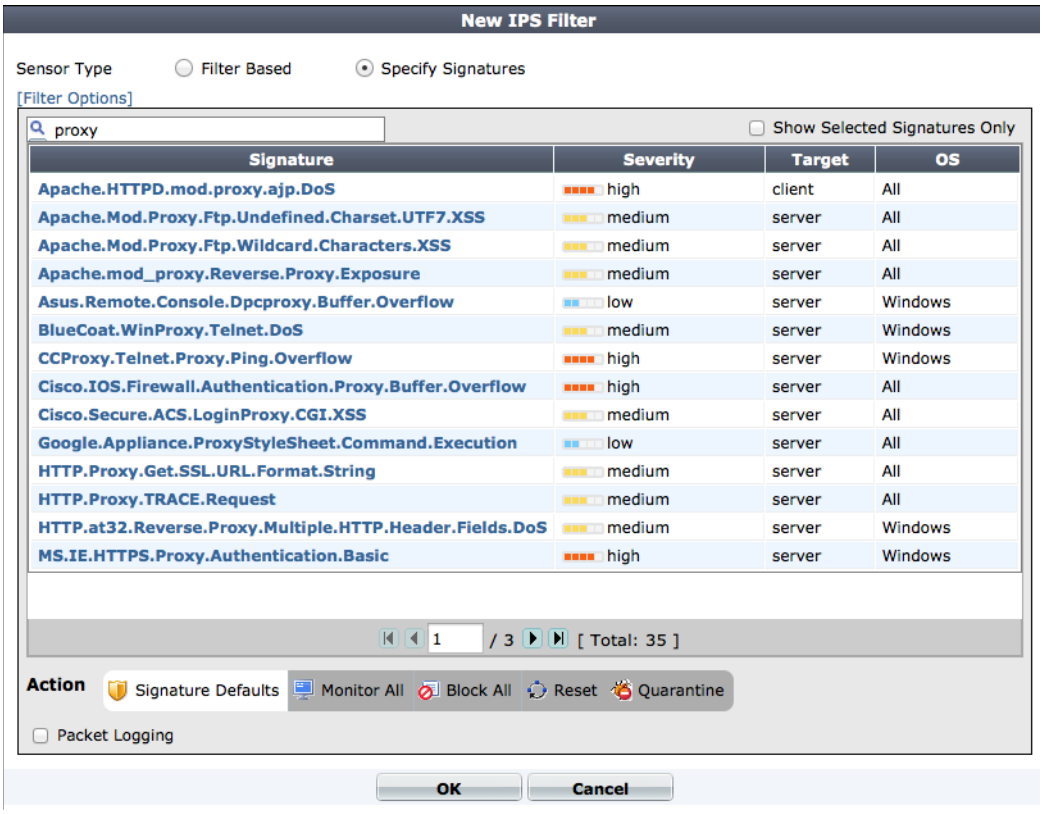
In FortiOS 5.0, it is much easier to sort through Fortinet's thousands of application definitions and IPS signatures to find the ones that you want to add to Application Control and IPS sensors. The creation pages for both of these features include filters for severity, category, popularity, technology and risk.

Figure 29: Application list filtering



You can also search through the application or signature list by name.

Figure 30:IPS signatures search example



Custom Application Control signatures and IPS signatures

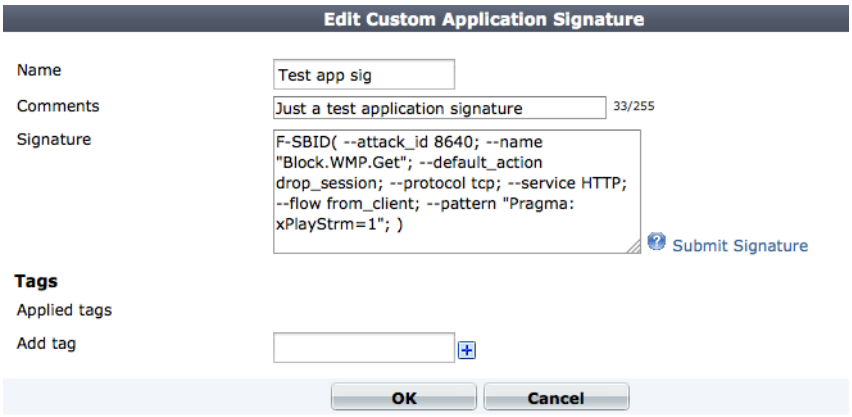
The application control and IPS signatures provide coverage for most applications and network vulnerabilities. You can extend the coverage by adding custom application signatures and custom IPS signatures.

You add custom application signatures by going to *Security Policies* > *Application Control* > *Application List* and selecting *Create New*.

You add custom IPS signatures by going to *Security Policies* > *Intrusion Protection* > *IPS Signatures* and selecting *Create New*.

Custom application signatures and custom IPS signatures use the same syntax. See the *UTM Guide* for a description the signature syntax.

Figure 31: Example custom application signature



Use the following command to add a custom application control signature.

```
config application custom
  edit New-custom-sig
    set signature F-SBID( --attack_id 8640; --name "Block.WMP.Get";
        --default_action drop_session; --protocol tcp; --service
        HTTP; --flow from_client; --pattern "Pragma: xPlayStrm=1";
        )
    end
```

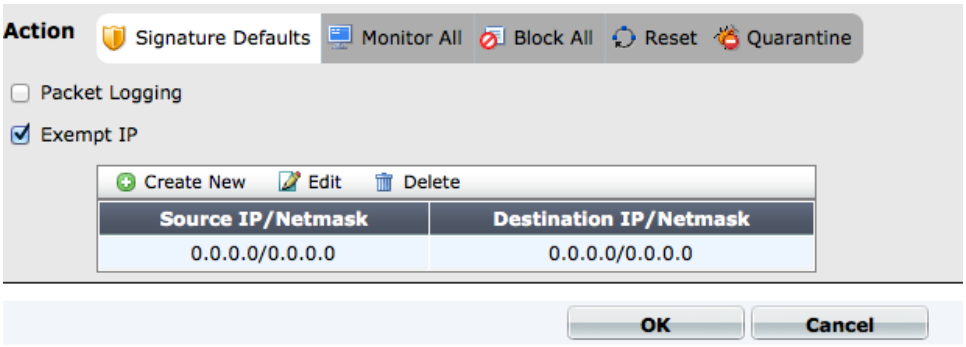
Use the following command to add a custom IPS signature.

```
config ips custom
  edit New-custom-sig
    set signature F-SBID( --attack_id 8640; --name "Block.WMP.Get";
        --default_action drop_session; --protocol tcp; --service
        HTTP; --flow from_client; --pattern "Pragma: xPlayStrm=1";
        )
    end
```

Exempting IP addresses from IPS

IPS filters can be configured so that signatures are not applied to traffic from specific IP addresses. To exempt an IP address, a filter must be created with the *Sensor Type* set to *Specify Signatures*. *Exempt IP* can then be enabled and the necessary exemptions configured using Source and Destination IPs.

Figure 32: Exempting IP addresses from IPS



Flow-based inspection improvements

If your FortiGate unit supports flow-based scanning, you can choose to select flow-based instead of proxy scanning. Flow-based scanning uses the FortiGate IPS engine to examine network traffic as it passes through the FortiGate unit without using a proxy to buffer and potentially change packets.

In FortiOS 5.0, flow-based inspection has been extended to email filtering. The following sections contain information about additional flow-based scanning improvements.

Configuring SSL inspection for flow-based and proxy protection

FortiOS 5.0 fully supports flow-based inspection of SSL sessions. This means that HTTPS, IMAPS, POP3S, SMTPS and FTPS traffic can now be decrypted and inspected by IPS and application control and flow-based antivirus, web filtering and email filtering.

FortiOS 5.0 continues to fully support proxy inspection of SSL sessions. In FortiOS 5.0, configuring proxy SSL inspection has changed as described below.

To enable proxy or flow-based inspection of SSL sessions, you must add an SSL/SSH Inspection profile to a security policy. You can configure SSL/SSH inspection profiles to inspect HTTPS, SMTPS, POP3S, IMAPS and FTPS traffic, as well as SSH traffic. You can configure the profile to control which SSL protocols to inspect, the ports to inspect for each protocol and the certificate to use with SSL sessions.

To apply proxy virus scanning and web filtering to HTTPS, IMAPS, POP3S, SMTPS and FTPS sessions

1. Go to *Policy* > *Policy* > *SSL/SSH Inspection* and create or edit an SSL/SSH inspection profile.
2. Under *SSL Inspection Options* select the CA certificate to use for SSL sessions. You can import a new certificate or use one already imported into the FortiGate unit.
3. Under enable the SSL protocols that you want to inspect and set the ports to inspect for each protocol.
4. Configure other settings as required and select *Apply* to save your changes.
5. Go to *Policy* > *Policy* > *Policy* and create a new or edit a policy that accepts the SSL traffic to be inspected.
6. Under *Security Profiles,* turn on *AntiVirus* and *Web Filter* and select profiles for them.
7. Turn on *SSL/SSH Inspection* and select the SSL/SSH inspection profile that you configured.
8. Select OK.

To apply flow-based virus scanning and web filtering and application control to HTTPS, and POP3S sessions

This example describes adding factory default antivirus, web filtering, application control and SSL/SSL profiles to a security policy that accepts HTTPS and POP3S traffic to apply flow-based virus scanning, web filtering and application control to the HTTPS and POP3S traffic accepted by the security policy.

1. Go to *Policy* > *Policy* > *Policy* and create or edit a policy that accepts the HTTPS and POP3S traffic to be inspected.
2. Under *Security Profiles,* turn on *AntiVirus* and select the *AV-flow* profile.
3. Turn on *Web Filter* and select the *web-filter-flow* profile.
4. Turn on *Application Control* and select the *default* profile.
5. Turn on *SSL/SSH Inspection* and select the *default* profile.
6. Select *OK*.

Explicit web Proxy Extensions – SSL inspection, IPS, Application Control, and flow-based antivirus, web filtering and DLP

FortiOS 5.0 fully supports SSL inspection of explicit web proxy traffic. This means that HTTPS traffic accepted by the explicit web proxy can now be subject to deep inspection for antivirus, web filtering and DLP.

FortiOS 5.0 also fully supports flow-based inspection of explicit web proxy traffic. This includes full support for IPS and application control, as well as flow-based virus scanning and web filtering for HTTP, HTTPS and FTP over HTTP traffic.

SSL content inspection and flow-based inspection are added to explicit web proxy sessions by enabling Security Profiles in a security policy that accepts web-proxy traffic and then selecting profiles that implement flow-based inspection for the features you need.

The explicit FTP proxy and the IPv6 explicit web proxy do not support SSL inspection or IPS, application control, and flow-based antivirus, web filtering and DLP.

Replacement messages for flow-based web filtering of HTTPS traffic

FortiOS 5.0 now supports replacement messages for flow-based HTTPS web filtering. Flow-based HTTP and HTTPS web filtering send the same replacement message as proxy web filtering. For FortiGuard web filtering, the replacement message is the *FortiGuard Block Page* and for URL web filtering, the replacement message is the *URL Block Page*. To edit replacement messages, go to *System* > *Config* > *Replacement Messages*.

DNS web filtering

A DNS request is typically the first part of any new session to a new website. DNS web filtering takes advantage of this by including the web site category in DNS responses. When a FortiGate unit resolves a URL, it receives a rating in addition to the IP address of the website.

DNS Web filtering uses the same categories as FortiGuard Web Filtering and requires you to configure your FortiGate unit to use FortiGuard DNS as its DNS Server. DNS web filtering is lightweight in terms of resource usage because it doesn't involve any actual content inspection.

DNS web filtering includes reduced functionality compared to proxy and flow-based web filtering. DNS web filtering does not support:

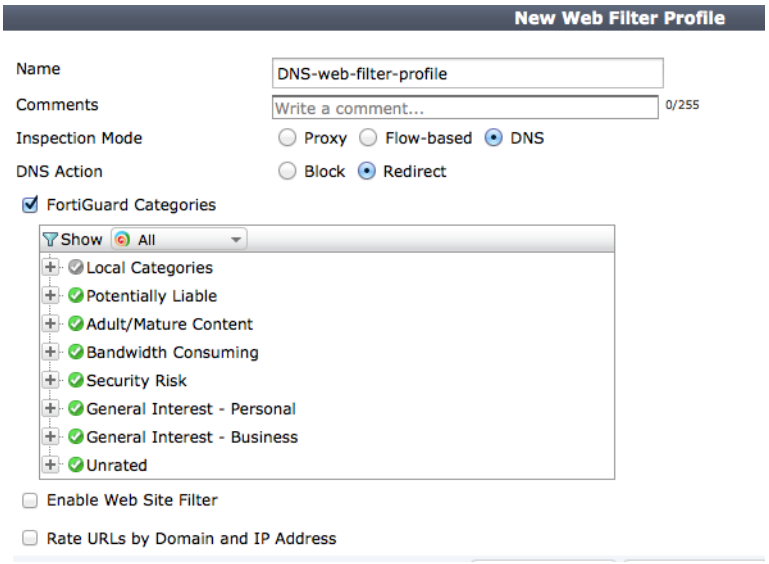
- Quotas
- Setting web filter categories to Warning or Authenticate (Allow, Monitor and Block are supported)
- Safe Search
- URL only scanning for HTTPS
- Advanced filtering options such as web content filtering, web resume download blocking, blocking invalid URLs, HTTP post action options, Java applet filtering, ActiveX filtering, cookie filtering, image rating, allowing websites when a rating error occurs and blocking HTTP redirects by rating

To configure your FortiGate unit to use DNS web filtering, start by going to *System* > *Network* > *DNS* and under *DNS Settings*, make sure *Use FortiGuard Servers* is selected and select *Apply*.

Go to *Security Profiles* > *Web Filter* > *Profiles* and edit a web filtering profile or create a new one. Set *Inspection Mode* to DNS. Then you can set *DNS action* to *Block* or *Redirect*. If you select *Redirect*, every time a web page is blocked by DNS web filtering the URL is re-directed to a web page on the FortiGuard network that displays a block message. If you select *Block,* the page is blocked and the user's web browsers display an error message or the connection attempt will time out.

Set the FortiGuard web filtering categories as required. You can configure DNS web filtering to block, allow and monitor web pages in each FortiGuard category. Select *Apply* to save the profile.

Figure 33:DNS web filtering profile



Go to *Policy* > *Policy* > *Policy* and create or edit a security policy, enable web filtering and select the web filtering profile that you configured for DNS web filtering.

All traffic HTTP accepted by the policy will be inspected by DNS web filtering.

FortiGuard Web Filter quotas can be set based on traffic volume

In FortiOS 5.0, FortiGuard web filter quotas can now set based on the amount of traffic as well as time.

You can add traffic quotas to a web filter profile from the CLI. The following command shows how to add a quota of 20 GB for bandwidth consuming web sites. These command assumes you have already set up the profile to monitor, warn or require authentication for bandwidth consuming web sites (category g04).

```
config webfilter profile
  edit default
    config ftgd-wf
      config quota
        edit 0
          set category g04
          set type traffic
          set unit GB
          set value 20
      end
    end
  end
```

Customizing the authentication replacement message for a FortiGuard web filter category

FortiOS 5.0 allows you to customize the replacement message that appears for a specific FortiGuard Web Filtering category. You do this by editing a Web Filter profile, right clicking on a FortiGuard Web Filtering category, selecting *Authenticate* and selecting a user group. Then right-click on the category again and select *Customize*.

A blank customize replacement message window appears and you can create the custom replacement message. Select *Save* and close the replacement message editor. The selected category has an Authenticate icon next to it. You can select this icon to edit the replacement message.

Saving the message creates a custom replacement message group. If you go to *System* > *Config* > *Replacement Messages Group* and open the replacement message group called *web-filter-default* you can find a *Custom Messages* category that contains the new replacement message.

YouTube Education Filter implemented in Web Filtering Profiles

You can add your organization's YouTube education filter to a web filtering profile. The Educational filter will be implemented on all YouTube sessions accepted by the security policy that the web filter profile is added to. This makes it easier to allow your users to only access educational YouTube content while blocking content not considered educational.

To add a YouTube eduction filter

1 Go to *Security Profiles* > *Web Filter* > *Profiles* and edit a web filter profile.

2 Select *Enable Safe Search* > *YouTube Education Filter* and enter the YouTube education filter code.

3 Select Apply to save the changes to the web filter profile.

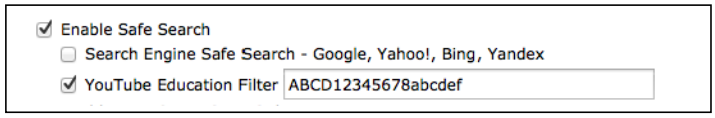
4 Go to *Policy* > *Policy* > *Policy* and edit the security policy that allows users to access the Internet.

5 Select Security Profiles.

6 Select *Enable Web Filter* and select the web filter profile that includes the YouTube education filter.

7 Select OK to save the security policy.

Figure 34: Adding a YouTube education filter code to a web filter profile



Use the following CLI command to add a YouTube education code to a web filter profile:

```
config webfilter profile
  edit youtube-EDU
    config web
      set safe-search youtube-edu
      set youtube-edu-filter-id "ABCD1234567890abcdef"
    end
  end
```

IPS hardware acceleration

FortiGate units with CPx and NPx processes can accelerate IPS performance by offloading pattern matching to the CPx or NPx processor. If your FortiGate hardware supports this feature the following CLI command will be available:

```
config ips global
  set hardware-accel-mode {engine-pick | none | CP-only | NP-only |
      NP+CP}
end
```

Where:

- `engine-pick`, let the IPS engine pick the best mode.
- `none`, hardware acceleration disabled.
- `CP-Only`, accelerate with content processors only.
- `NP-only`, accelerate with network processor only.
- `NP+CP`, accelerate with both network and content processors.

New SIP ALG features

FortiOS 5.0 includes the following new SIP ALG features:

- Inspecting SIP over SSL/TLS (secure SIP)
- Opening and closing SIP via and record-route pinholes
- Adding the original IP address and port to the SIP message header after NAT

Inspecting SIP over SSL/TLS (secure SIP)

Some SIP phones and SIP servers can communicate using SSL or TLS to encrypt the SIP signalling traffic. To allow SIP over SSL/TLS calls to pass through the FortiGate unit, the encrypted signalling traffic has to be unencrypted and inspected. To do this, the FortiGate SIP ALG intercepts, unencrypts and inspects the SIP packets. The packets are then re-encrypted and forwarded to their destination.

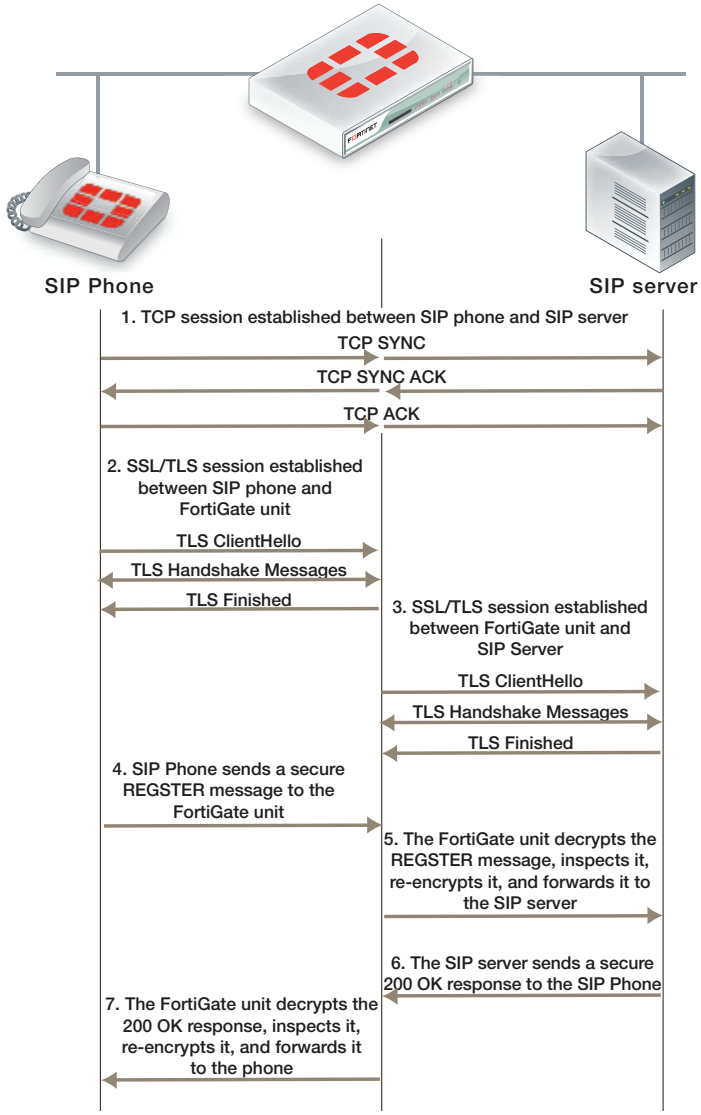
Normally SIP over SSL/TLS uses port 5061. You can use the following command to change the port that the FortiGate listens on for SIP over SSL/TLS sessions to port 5066:

```
config system settings
  set sip-ssl-port 5066
end
```

The SIP ALG supports full mode SSL/TLS only. Traffic between SIP phones and the FortiGate unit and between the FortiGate unit and the SIP server is always encrypted.

You enable SSL/TLS SIP communication by enabling SSL mode in a VoIP profile. You also need to install the SIP server and client certificates on your FortiGate unit and add them to the SSL configuration in the VoIP profile.

Figure 35:SIP over SSL/TLS between a SIP phone and a SIP server



Other than enabling SSL mode and making sure the security policies accept the encrypted traffic, the FortiGate configuration for SSL/TLS SIP is the same as any SIP configuration.

SIP over SSL/TLS is supported for all supported SIP configurations.

Adding the SIP server and client certificates

A VoIP profile that supports SSL/TLS SIP requires one certification for the SIP server and one certificate that is used by all of the clients. Use the following steps to add these certificates to the FortiGate unit. Before you start, make sure the client and server certificate files and their key files are accessible from the management computer.

1. Go to *System* > *Certificates* > *Local Certificates* and select *Import.*
2. Set *Type* to *Certificate*.
3. Browse to the *Certificate file* and the *Key file* and select *OK*.
4. Enter a password for the certificate and select *OK*.

   The certificate and key are uploaded to the FortiGate unit and added to the *Local Certificates* List.
5. Repeat to upload the other certificate.

The certificates are added to the list of Local Certificates as the filenames you uploaded. You can add comments to make it clear where the certificate is from and how it is intended to be used.

Adding SIP over SSL/TLS support to a VoIP profile

Use the following commands to add SIP over SSL/TLS support to the default VoIP profile. The following command enables SSL mode and adds the client and server certificates and passwords (the same ones you entered when you imported the certificates):

```
config voip profile
  edit default
    config sip
      set ssl-mode full
      set ssl-client-certificate "Client_cert"
      set ssl-server-certificate "Server_cert"
      set ssl-auth-client "check-server"
      set ssl-auth-server "check-server-group"
  end
end
```

Other SSL mode options are also available:

`ssl-send-empty-frags {disable | enable}`	Enable to send empty fragments to avoid CBC IV attacks. Compatible with SSL 3.0 and TLS 1.0 only. Default is `enable`.
`ssl-client-renegotiation {allow | deny | secure}`	Control how the ALG responds when a client attempts to renegotiate the SSL session. You can allow renegotiation or block sessions when the client attempts to renegotiate. You can also select `secure` to reject an SSL connection that does not support RFC 5746 secure renegotiation indication. Default is `allow`.

`ssl-algorithm {high | low | medium}`	Select the relative strength of the algorithms that can be selected. You can select `high`, the default, to allow only AES or 3DES, `medium`, to allow AES, 3DES, or RC4 or `low`, to allow AES, 3DES, RC4, or DES.
`ssl-pfs {allow | deny | regqure}`	Select whether to `allow`, `deny`, or `require` perfect forward secrecy (PFS). Default is `allow`.
`ssl-min-version {ssl-3.0 | tls-1.0 | tls-1.1}`	Select the minimum level of SSL support to allow. The default is `ssl-3.0`.
`ssl-max-version {ssl-3.0 | tls-1.0 | tls-1.1}`	Select the maximum level of SSL support to allow. The default is `tls-1.1`.

Opening and closing SIP via and record-route pinholes

If `open-via-pinhole` is disabled (the default setting), the FortiGate unit does not open pinholes for Via messages. You can enable `open-via-pinhole` so that the FortiGate unit opens pinholes for Via messages. In previous versions of FortiOS, this option was `reg-diff-port`.

If `open-record-route-pinhole` is enabled (the default setting), the FortiGate unit opens pinholes for Record-Route messages. You can disable `open-record-route-pinhole` so that the FortiGate unit does not open pinholes for Record-Route messages.

Usually you would want to open these pinholes. Keeping them closed may prevent SIP from functioning properly through the FortiGate unit. However, they can be disabled for interconnect scenarios (where all SIP traffic is between proxies and traveling over a single session). In some cases, these settings can also be disabled in access scenarios if it is known that all users will be registering regularly so that their contact information can be learned from the register request.

You may also want to prevent pinholes from being opened to avoid creating a pinhole for every register or non-register request. Each pinhole uses additional system memory, which can affect system performance if there are hundreds or thousands of users, and requires refreshing that can take a relatively long amount of time if there are thousands of active calls.

Adding the original IP address and port to the SIP message header after NAT

In some cases, your SIP configuration may require that the original IP address and port from the SIP contact request is kept after NAT. For example, the original SIP contact request could include the following:

```
Contact: <sip:0150302438@172.20.120.110:5060>;
```

After the packet goes through the FortiGate unit and NAT is performed, the contact request could look like the following (the IP address translated to a different IP address and the port to a different port):

```
Contact: <sip:0150302438@10.10.10.21:33608>;
```

You can enable `register-contact-trace` in a VoIP profile to have the SIP ALG add the original IP address and port in the following format:

```
Contact: <sip:0150302438@<nated-ip>:<nated-port>;o=<original-ip>:
    <original-port>>;
```

So the contact line after NAT could look like the following:

```
Contact: <sip:0150302438@10.10.10.21:33608;o=172.20.120.110:5060>;
```

Enter the following command to enable keeping the original IP address and port:

```
config voip profile
  edit Profile_name
    config sip
      set register-contract-trace enable
  end
```

DLP watermarking

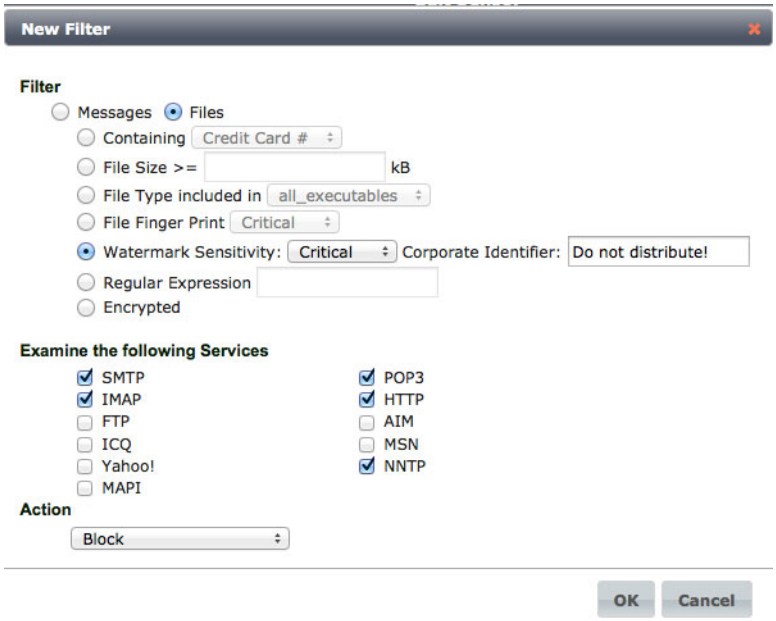
DLP watermarking involves using DLP to filter files that pass through the FortiGate unit and contain a corporate identifier (a text string) and a sensitivity level (Critical, Private and Warning) hidden in a watermark. Watermarked files have this information applied in a way that is not visible to the user. DLP watermarking requires a FortiGate unit with a hard disk or flash disk.

You must use the Fortinet watermarking client to apply a watermark to a file. Files should be watermarked before they are distributed. Then, with DLP watermarking enabled, your FortiGate unit can track and optionally block watermarked files that pass through it.

To configure DLP to filter for watermarked files, go to *Security Profiles* > *Data Leak Prevention* > *Sensors* and create or edit a DLP sensor. Add a filter to the sensor and set *Filter* to *Files*. Then select *Watermark Sensitivity* and select *Critical*, *Private* or *Warning*. Then enter the *Corporate Identifier*. The corporate identifier is a case-sensitive text string that must exactly match the corporate identifier text string added by the watermarking client.

Select the services in which to look for watermarked files. Usually you would choose all of the email protocols active on your network and HTTP. Then set the action for the watermark filter. When DLP finds a file with a watermark that matches the filter, the action selected in the filter is performed. Actions include writing a log message, blocking the file or quarantining the user, IP address or interface.

Figure 36:DLP filter configuration using a watermark



Files can have multiple watermarks in them. The FortiGate unit only has to find one match in a file for DLP watermarking to match it and it will ignore watermarks that don't match. Files without watermarks are ignored by DLP watermarking.

Fortinet watermarking utility

Watermarking uses a digital pattern to mark a file as being proprietary to a specific company. Fortinet has a utility that will apply a digital watermark to any file except a .txt file. The utility adds a small (around 100 bytes) pattern to the file that is recognized by the DLP Watermark filter. This pattern is invisible to the end user.

Currently, FortiGate DLP only works with Fortinet's watermarking client. When watermarking a file, it should be verified that the pattern matches up to a DLP category. Before planning to use watermarking software, it is always best to verify that the software will work with your OS and file types. At the time of writing this document the utility was only available with the current version of FortiExplorer for Windows or through using the CLI for Linux.

Installation of the watermarking client on Linux

Add the watermark file to a location on the system that is in the $PATH

To see what the path is use the command

```
~$ echo $PATH
```

Example results:

```
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/ga
    mes
```

for example you could move or copy the file to the :/bin directory.

Permissions on the watermark file

Check the existing permissions:

The command in Linux for listing file along with the permissions is:

```
ls -l
```

Run the check to see if the permission status. The results may be something along these lines:

```
-rw-r--r-- 1 root root 2053868 Jan 10 11:44
    fortinet-watermark-linux.out
```

You will see that in this case it has no executable permissions

To change the permissions on the watermark file:

It will be assume for this command that the utility is in the bin directory and that you have ownership level access.

```
/bin# chmod o+x /bin/ fortinet-watermark-linux.out
```

To verify the change:

```
/bin# ls -l wa*
-rw-r--r-x 1 root root 2053868 Jan 10 11:44
    fortinet-watermark-linux.out
```

You can see how the x for executable has been added to the permissions for the others group.

Syntax of the watermarking client on Linux

The tool is executed in a Linux environment by passing in files or directories of files to insert a watermark.

USAGE:

```
fortinet-watermark-linux.out <options> -f <file name> -i <identifier>
    -l <sensitivity level>
fortinet-watermark-linux.out <options> -d <directory> -i <identifier>
    -l <sensitivity level>
```

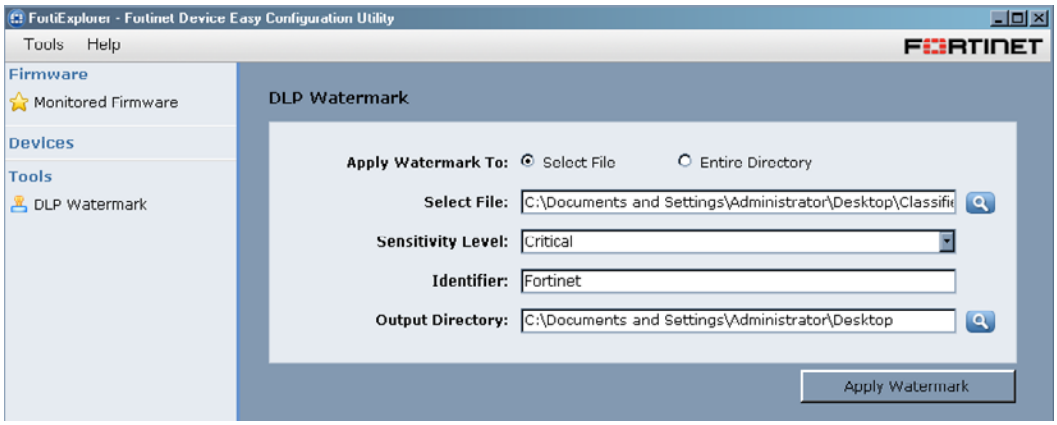
Options:

```
-h print help
-v verbose information
-I inplace watermarking (don't copy file)
-o output directory
-e encode <to non-readable>
-a add additional watermark (by default replaces watermarks existing
     watermarks)
-D delete all watermarks
```

Using the watermarking client with Windows

The watermarking client is now part of FortiExplorer in Windows, appearing in the Tools menu. Using the client, you can apply a watermark to any files you wish to track and possibly block using DLP.

Figure 37: The Fortinet watermarking client in Windows



Using the watermarking client with Linux

If you are in your home directory and you want to watermark a file in the Documents directory, you could plan out the command like this:

watermark [because that is the executable to be used]

-v [so that you can get as much feedback as possible]

-I [because you don't want a new file you just want to watermark the existing one]

-f [because you only want to change the one file not the entire directory]

filename.pdf [the name of the file]

-i 123456 [to set the identifier to 123456 - this is a required setting

-l Private [to set the sensitivity level to "Private"]

Now at the command prompt enter all of these components in order:

```
~/Documents$ fortinet-watermark-linux.out -v -I -f filename.pdf -i
     12345 -l Private
Creating watermark.  Pattern:
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=identifier=12345
     sensitivity=Private=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
Watermarking file: 'filename.pdf'
Inserted watermark size 148
<command prompt>:~/Documents$
```

SSH inspection

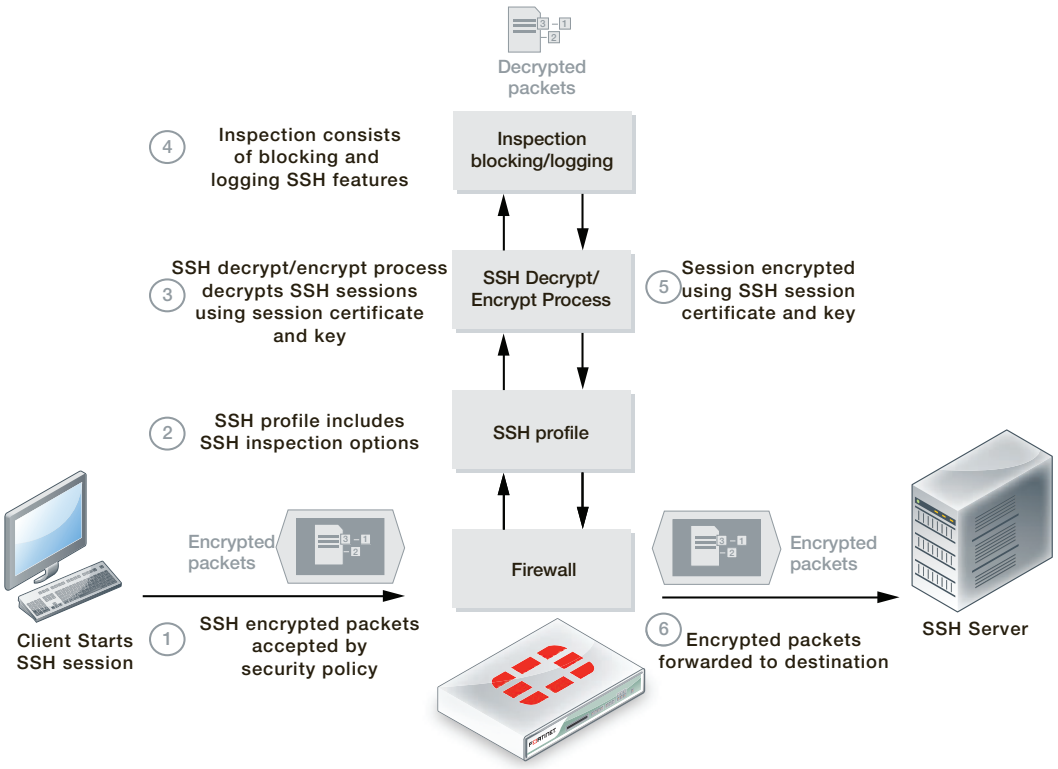
FortiOS 5.0 includes a new SSH proxy, available on selected models, that supports decrypting and inspecting SSH sessions to block or log the following:

- SSH remote execution
- Port forwarding
- SSH remote shell
- x11 server forwarding

Similar to SSL content inspection, the SSH proxy intercepts the SSH key exchange between the SSH client and server when an SSH session is being set up. All traffic that is part of the SSH session is decrypted by the SSH proxy and SSH inspection features are applied according to the SSH profile in the security policy that accepts the SSH traffic. After inspection, the session is re-encrypted and forwarded to the recipient.

SSH inspection is enabled by default in a SSL/SSH inspection profile.

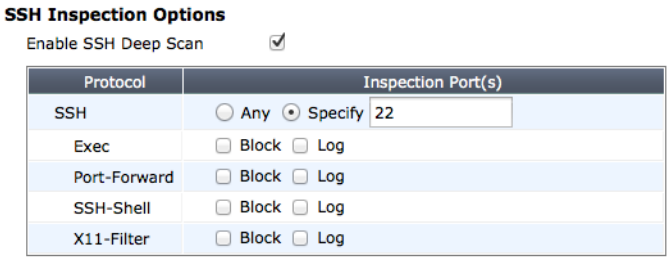
Figure 38:SSH inspection



To configure SSH inspection, go to *Policy* > *Policy* > *SSL/SSH Inspection* and create or edit an SSL/SSH Inspection profile and ensure that *SSH Inspection Options* are enabled. Then configure the port or ports to look for SSH traffic on. The default port is 22 but you can add more. You can then block or log Exec commands, port-forwarding, SSH shells, and X11 FIlters.

Then add this profile to security policy that accepts SSH traffic. Enable the required Security Profiles in the policy.

Figure 39: Configuring SSL Inspection Options



From the CLI:

```
config firewall profile-protocol-options
  edit new-profile
    config ssh
      set port <number> <number> ... (default is port 22)
      set inspect-all {enable | disable}
      set options {allow-invalid-server-cert | ssl-ca-list }
      set oversize-limit <size>
      set block {exe | port-forward | ssh-shell | x11-filter}
    end
```

Optimizing SSL encryption/decryption performance

By default, FortiGate units handle SSL decryption/encryption using the SSL functionality built into their FortiASIC processors. In situations where the FortiGate unit processes large amounts of SSL traffic and has more than 4 CPUs, you may be able to optimize SSL encryption/decryption performance by changing how SSL processing is distributed to the CPUs. You can also use the following command to specify the number of CPUs to use for SSL processing (in the command, CPU is called an SSL worker):

```
config system global
  set optimize-ssl {enable | disable}
  set ssl-worker-count <worker-count>
end
```

The `<worker-count>` is the number of CPUs. The range depends on the number of CPUs in the FortiGate model (this feature only works for FortiGate units with 4 or more CPUs).

You can use the following command to display information about each CPU running in your FortiGate unit:

```
get hardware cpu
```

The command output numbers the CPUs starting at 0. For example, a FortiGate-5001B contains 8 CPUs and the command output for this model contains information about all 8 CPUs numbered 0 to 7. Here is the first few output lines for CPU 7:

```
...
processor       : 7
vendor_id       : GenuineIntel
cpu family      : 6
model           : 14
model name      : Intel(R) Xeon(R) CPU           C5528  @ 2.13GHz
stepping        : 4
cpu MHz         : 2128.072
...
```

If your FortiGate unit includes multiple CPUs and you want to improve SSL performance, use the following command to begin distributing SSL decryption/encryption to 4 CPUs:

```
config system global
  set optimize-ssl enable
  set ssl-worker-count 4
end
```

Monitor FortiGate performance and if SSL performance improves without affecting other performance, you can either maintain this configuration or add another CPU to the configuration (if one is available). Continue in this manner until you achieve optimum performance for your FortiGate unit.

Continue monitoring performance in case you have to change this setting due changes in your network traffic patterns.

Authentication: users and devices

The FortiGate authentication umbrella has been expanded from just user authentication (or user identity) to encompass device identification and client reputation. As well, endpoint control and the vulnerability scanner have become part of FortiOS 5.0 user and device detection, identification and authentication.

Endpoint control and vulnerability scanner changes are described in this chapter. For information about device identification, see "FortiOS and BYOD" on page 98. For information about client reputation, see "Client Reputation" on page 106.

New authentication features described in this chapter include:

- User authentication menu changes
- User identity policy changes
- Authentication-based routing
- Secondary and tertiary RADIUS, LDAP, and TACAS+ servers
- FortiToken two-factor authentication and FortiToken Mobile
- SSO using a FortiAuthenticator unit
- SSO with Windows AD or Novell
- Citrix Agent support for Single Sign On
- Configuring guest access
- Vulnerability Scanning

User authentication menu changes

The user authentication part of FortiOS is seeing major changes for FortiOS 5.0. To begin, the *User* section of the web-based manager has been renamed *User & Device*. All previously available user authentication features are still available but the menu structure has changed to include device identification, the vulnerability scanner, endpoint control, and client reputation:

- Go to *User & Device* > *User* to configure users, user groups, and guest users ("Configuring guest access" on page 91)
- Go to *User & Device* > *Authentication* to configure single sign-on and add RADIUS, LDAP, and TACACS+ servers
- Go to *User & Device* > *Two-factor Authentication* to configure support for two-factor authentication using FortiToken ("FortiToken two-factor authentication and FortiToken Mobile" on page 86)
- Go to *User & Device* > *Vulnerability Scan* to configure and operate the FortiGate vulnerability scanner ("Vulnerability Scanning" on page 94)
- Go to *User & Device* > *Monitor* to view the firewall and banned user authentication lists

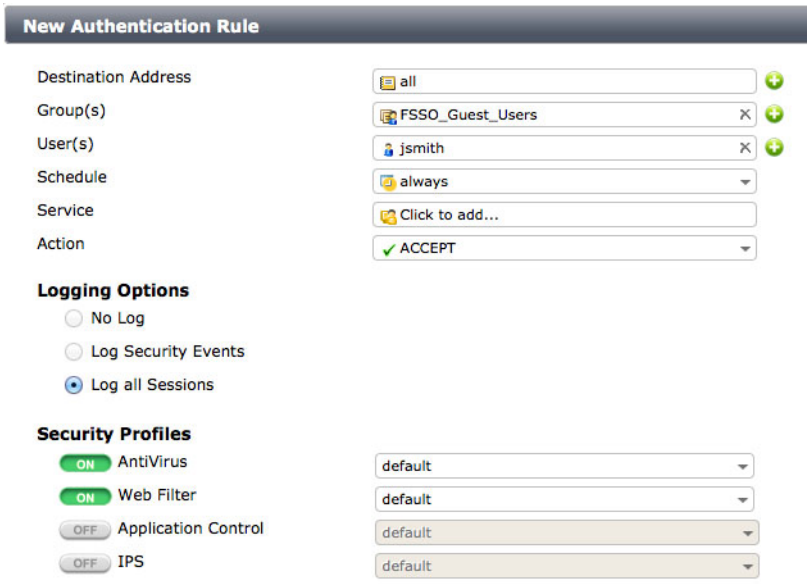
User identity policy changes

The steps for adding user identity-based policies have changed. To add a user identity based policy go to *Policy* > *Policy* > *Policy* and create a new security policy. Select the *Firewall* policy type and the *User Identity* subtype. Select the incoming and outgoing interfaces and source addresses. Configure other features such as NAT and so on.

Then select *Create New* to add user authentication rules to the policy. User authentication rules include the destination addresses, user groups and or individual users, schedule, service, action, logging, and UTM security profiles.

You select the destination address separately for each authentication rule. This means that you can apply different features to different user groups depending on the destination address.

Figure 40: Adding a user authentication rule



Authentication-based routing

FortiOS 5.0 supports authentication-based routing by creating an identity-based route that associates a user group with one or more routes. This identity-based route is then added to a security policy and all traffic from users authenticated by this user group is routed to the gateway. This feature is configured from the CLI and can be useful for MSSPs who need to route users from different organizations to different Internet gateways.

Enter the following command to add an identity-based route that routes all traffic from users in the company1-user-group and the company2-user-group user groups out the wan1 interface to a next-hop router with IP address 172.20.120.2:

```
config firewall identity-based-route
  edit new-id-route
    config rule
      edit 1
        set gateway 172.20.120.2
        set device wan1
        set groups company1-user-group company2-user-group
      end
    end
```

Enter the following command to add the identity-based route to a security policy:

```
config firewall policy
  edit 1
    ...
    set identity-based enable
    set identity-based-route new-id-route
    ...
  end
```

Secondary and tertiary RADIUS, LDAP, and TACAS+ servers

You can now add secondary and tertiary servers to RADIUS, LDAP, and TACAS+ remote authentication server configurations. When you add a secondary server, the FortiGate unit will contact the secondary server only if the primary server is unreachable. The FortiGate unit will only contact the tertiary server if the both the primary and secondary servers are unreachable.

Enter the following command to add up to three servers to a RADIUS server configuration. Specify a domain name or IP address for each server as well as the server secret. In the following example, the RADIUS servers are at IP addresses 172.20.120.10, 172.20.120.20, and 172.20.120.30:

```
config user radius
  edit new-radius-server
    set server 172.20.120.10
    set secret 1st-secret
    set secondary-server 172.20.120.20
    set secondary-secret 2nd-secret
    set tertiary-server 172.20.120.30
    set tertiary-secret 3rd-secret
  end
```

Enter the following command to add up to three servers to an LDAP server configuration. Specify a domain name or IP address for each server. Other than the domain name or password, the secondary and tertiary servers must use the same port and LDAP settings such as the cnid and username. In the following example, the LDAP servers are at IP addresses 192.168.10.10, 192.168.10.20, and 192.168.10.30:

```
config user ldap
  edit "test-ldap"
    set server "192.168.10.10"
    set cnid "exAccountName"
    set dn "dc=americas,dc=example,dc=net"
    set port 3268
    set type regular
    set username "CN=example,OU=Service
         Accounts,OU=Admins,DC=example,DC=csplc,DC=net"
    set password ENC AAAEAOZh5R5/oqYeUVkO2OOKh9QV6DAVZoAjbv0sonh
    set member-attr "ASCCGKraftFortinetVPNInternalUsers"
    set secondary-server "192.168.10.20"
    set tertiary-server "192.168.10.30"
  end
```

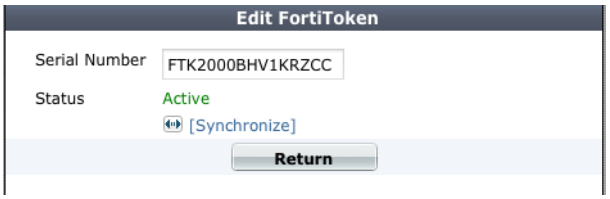
Enter the following command to add up to three servers to an TACAS+ server configuration. Specify a domain name or IP address and key for each server. In the following example, the TACAS+ servers are at IP addresses 10.10.10.10, 10.10.10.20, and 10.10.10.30:

```
config user tacacs+
  edit "test-tacacs"
    set server "10.10.10.10"
    set key ENC
         2OG/F6wocz2/CpE3eHIJs/Qt8gZsXgeNkQCuTxPWPeBk6BXDu8luM
    set secondary-server "10.10.10.20"
    set secondary-key ENC 2OG/F6wocz2/CpE3eHIJs/Qt8gZ
    set tertiary-server "10.10.10.30"
    set tertiary-key ENC 2OG/F6wocz2/CpE3eHIJs/Qt8gZ
    next
  end
```

FortiToken two-factor authentication and FortiToken Mobile

The web-based manager provides improved management of FortiToken devices. The status of each current FortiToken device is listed under *User & Device* > *Two-factor Authentication* > *Fortitokens*. You can also resynchronize FortiToken devices that have gone out of sync. You can also enter new FortiToken devices individually or by importing a list of FortiToken serial numbers in a text file.

Figure 41: View status and synchronize a FortiToken



Configuring FortiToken mobile soft token support

FortiOS 5.0 adds support for FortiToken Mobile, a Fortinet application that enables you to generate One Time Passwords (OTPs) on a mobile device for FortiGate two factor authentication. The user's mobile device and the FortiGate unit must be connected to the Internet to activate FortiToken mobile. Once activated, users can generate OTPs on their mobile device without having network access.

FortiToken Mobile is available for iOS and Android devices from their respective Application stores. No cellular network is required for activation.

The latest FortiToken Mobile documentation is available from the FortiToken page of the Fortinet Technical Documentation website.

To use FortiToken Mobile, a user needs to install the application on their mobile device and then activate a token. After the token is activated, the user can begin to generate OTPs on their mobile device.

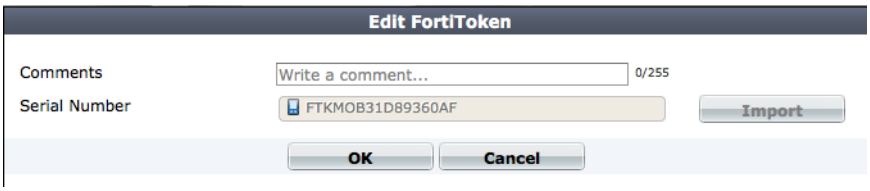
Two free trial tokens are included with every registered FortiGate unit. Additional tokens can be purchased from your reseller or from Fortinet.

You can generate the two free tokens from the FortiGate CLI by entering the following command:

```
execute fortitoken-mobile import 0000-0000-0000-0000-0000
```

This command adds two FortiToken mobile entries to the FortiGate configuration. To view them, go to *User & Device* > *Two-factor Authentication* > *Fortitokens* and open the *MobileToken* list and edit one of the entries.

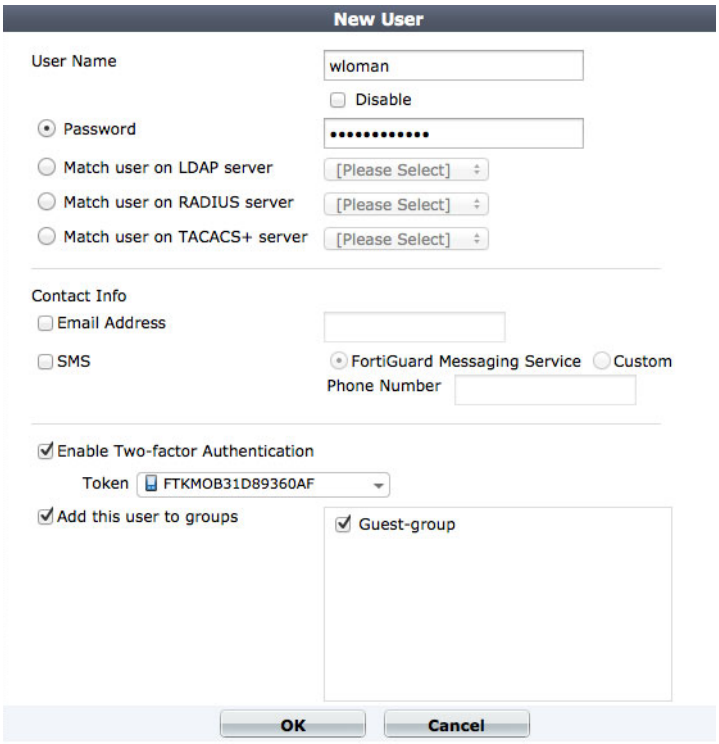
Figure 42: Example free FortiToken Mobile token



To assign a token to a user, go to *User & Device* > *User* > *User Definition* and either add a new user or select the user to assign the token to. Configure the user as required and select *Enable Two-factor Authentication*. Select the token to associate with the user.

Select *OK* to assign the token to the user. If you have added the user's email address or configured SMS settings and configured your FortiGate unit to send email or send SMS messages, the FortiGate unit sends the user an activation code. (To configure your FortiGate unit to send email or SMS messages go to *System* > *Config* > *Messaging Servers*.)

Figure 43: Assigning a FortiToken Mobile token to a user



If for some reason you cannot send the activation code to the user through email or an SMS message, or would rather send the activation code by other means specific to your operation, you can view the activation code from the CLI. For example, for a token with serial number of FTKMOB28E0CA6018 you can enter the following commands:

```
config user fortitoken
  edit FTKMOB28E0CA6018
  get
  serial-number       : FTKMOB28E0CA6018
  activation-code     : 8F41F304
  activation-expire   : 604800
  comments            :
  license             : FTMTRIAL00001088
  status              : active
```

Send the activation-code (in this example, `8F41F304`) to the user. Following the instructions in the *FortiToken Mobile User Guide,* the user can activate their FortiToken Mobile application using this activation code.

The user's mobile device, as well as the FortiGate unit, must be connected to the Internet to complete the activation. When the activation is complete, the *Status* of the FortiToken Mobile token changes to *Provisioned* on the FortiGate unit.

SSO using a FortiAuthenticator unit

If you use a FortiAuthenticator unit in your network as a single sign-on agent:

- Users can authenticate through a web portal on the FortiAuthenticator unit.
- Users with FortiClient Endpoint Security installed can be automatically authenticated by the FortiAuthenticator unit through the FortiClient SSO Mobility Agent.

The FortiAuthenticator unit can integrate with external network authentication systems such as Windows Active Directory, Novell e-Directory, RADIUS and LDAP to gather user logon information and send it to the FortiGate unit.

User's view of FortiAuthenticator SSO authentication

There are two different ways users can authenticate through a FortiAuthenticator unit.

Users without FortiClient Endpoint Security - SSO widget

To log onto the network, the user accesses the organization's web page with a web browser. Embedded on that page is a simple logon widget. The SSO widget sets a cookie on the user's browser. When the user browses to a page containing the login widget, the FortiAuthenticator unit recognizes the user and updates its database if the user's IP address has changed. The user will not need to re-authenticate until the login expires, which can take up to 30 days.

Users with FortiClient Endpoint Security - FortiClient SSO Mobility Agent

All authentication is performed transparently with no request for credentials. IP address changes, such as those due to WiFi roaming, are automatically sent to the FortiAuthenticator unit. When the user logs off or otherwise disconnects from the network, the FortiAuthenticator unit is aware of this and deauthenticates the user.

The FortiClient SSO Mobility Agent, a feature of FortiClient Endpoint Security v5.0, must be configured to communicate with the appropriate FortiAuthenticator unit. After that, the agent automatically provides user name and IP address information to the FortiAuthenticator unit for transparent authentication.

Administrator's view of FortiAuthenticator SSO authentication

You can configure either or both of these authentication types on your network.

SSO widget

You need to configure the Single Sign-On portal on the FortiAuthenticator unit. Go to *SSO & Dynamic Polices* > *SSO* > *Login Portal* to do this. Copy the *Embeddable login widget* code for use on your organization's home page. Identity-based security policies on the FortiGate unit determine which users or groups of users can access which network resources.

FortiClient SSO Mobility Agent

Your users must be running FortiClient Endpoint Security v5.0 to make use of this type of authentication.

On the FortiAuthenticator unit, you need to enable *FortiClient Service* when you define the unit's secret key. Go to *SSO & Dynamic Policies* > *SSO* > *Options*. You need to provide your users the FortiAuthenticator IP address and secret key so that they can configure the FortiClient SSO Mobility Agent on their computers.

SSO with Windows AD or Novell

The FortiGate unit can authenticate users transparently based on their Windows Active Directory (AD) or Novell eDirectory privileges. This means that users who have logged on to the network are not asked again for their credentials to access network resources through the FortiGate unit, hence the term "Single Sign-On".

FSSO Collector agent and DC agent have been tested on Windows Server 2003, 2008 and 2012.

On a Microsoft Windows or Novell network, users authenticate with the Microsoft AD or Novell eDirectory at logon. It would be inconvenient if users then had to enter another username and password for network access through the FortiGate unit. FSSO agents installed on the network provide user information, such as IP address and user group memberships, to the FortiGate unit. Security policies on the FortiGate unit allow network access based on the user groups to which the user belongs.

There are several mechanisms for passing user authentication information to the FortiGate unit:

- FSSO Collector agent software installed on a Windows AD network monitors user logons and sends the required information to the FortiGate unit. The FSSO software can obtain this information by polling the AD domain controllers or by using an FSSO agent on each AD domain controller that monitors user logons in real time. New in FortiOS 5.0, a FortiGate unit can obtain group information directly from AD using Lightweight Directory Access Protocol (LDAP).
- On a Windows AD network, the FSSO software can also serve NT LAN Manager (NTLM) requests coming from client browsers (forwarded by the FortiGate unit) with only one or more Controller agents installed.
- FSSO eDirectory agent software installed on a Novell network monitors user logons and sends the required information to the FortiGate unit. The agent can obtain information from the Novell eDirectory using either the Novell API or LDAP.
- A FortiAuthenticator server can act as a replacement for the Collector agent in polling mode in a Windows AD network. FortiAuthenticator can also be configured with internal or external LDAP and RADIUS servers. For more information, see the *FortiAuthenticator Administration Guide*.

Citrix Agent support for Single Sign On

FortiOS 5.0 supports single sign on authentication for Citrix environments by installing a Citrix FSSO polling agent on the Citrix server, installing an FSSO collector on the network, and then configuring the FortiGate unit to get user credentials from the Citrix FSSO polling agent.

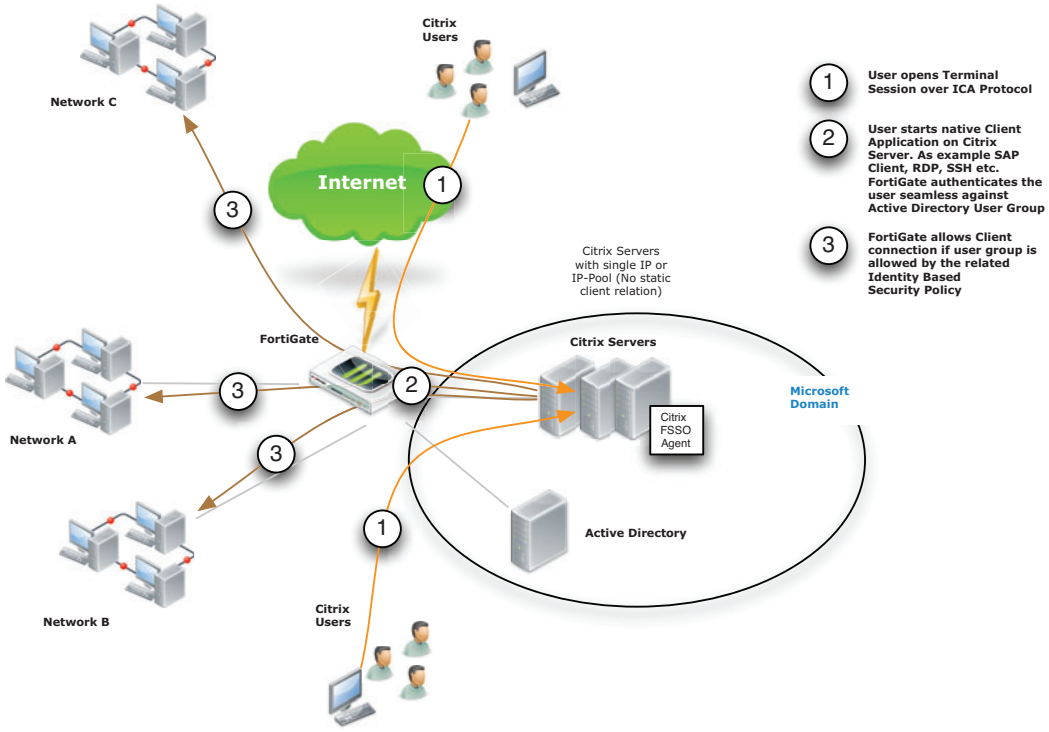
TSAgent running on the Citrix server XenAPP server version 6 has been tested with FSSO build0129 running Windows Server 2008.

Configuration steps include:

- Install the Fortinet Citrix FSSO agent on the Citrix server.
- Install the Fortinet FSSO collector on a server on the network.
- Add the Citrix FSSO agent to the FortiGate Single-sign-On configuration.
- Add Citrix FSSO groups and users to an FSSO user group.
- Add an FSSO identity-based security policy that includes the Citrix FSSO user groups.

After this configuration is complete, Citrix users credentials are made available to the FortiGate unit by the Citrix FFSO agent when a Citrix Terminal Session is started.When the user starts a client application (such as a web browser, SAP client, and so on), the user's session through the FortiGate unit is automatically authenticated and allowed by the FSSO identity-based security policy.

Figure 44: Example Citrix single sign on with FSSO network topology



Installing Citrix/Terminal Service Support Agent (TS Agent)

Install the Citrix/terminal service support agent on the Citrix terminal server, or other terminal, in the same was a you would install the FSSO agent on any platform.

1. Log into the server with an account that has administrator privileges and a password that does not expire.
2. Start the FSSO agent installer.

3. Following the installation wizard prompts.

   During the installation process:

   - the *Host IP Address* is The local IP of the Citrix or Terminal service server.
   - The *Fortinet SSO collector IP and port* is the IP and port of the FSSO collector.

4. Make sure that Launch DC Agent Install Wizard is selected and then select Finish to end the installation.

Installing the FSSO collector

There are no special requirements for installing the FSSO collector.

To enable single sign-on using polling mode

1. Go to *User & Device* > *Authentication* > *Single Sign-On* and select *Create New* to add a single sign-on server.
2. Select *Fortinet Single-Sign-On Agent*.
3. Enter the Name and the IP address or Name and password for the Citrix server.
4. Select *OK* to save the configuration.

Verifying the configuration

You can use the following diagnose commands to verify the configuration:

```
diagnose debug authd fsso list
diagnose debug application authd -1
diagnose firewall auth list
```

Configuring guest access

You can create many guest accounts at once using randomly-generated User IDs and passwords. This reduces administrator workload for large events.

User's view of guest access

1. The user receives an email, SMS message or printout from a FortiGate administrator listing a User ID and password.
2. The user logs onto the network with the provided credentials.
3. After the expiry time, the credentials are no longer valid.

Administrator's view of guest access

1. Create one or more guest user groups.

   All members of the group have the same characteristics: type of User ID, type of password, information fields used, type and time of expiry.

2. Create guest accounts using Guest Management.
3. Use captive portal authentication and select the appropriate guest group.

Creating guest management administrators

The guest management administrator can be a regular FortiGate administrator. Optionally, you can create administrator accounts that can perform only guest management. This type of administrator is also limited to specific guest user groups.

To create a guest management administrator

1. Go to *System* > *Admin* > *Administrators* and create a regular administrator account.
   For detailed information see the System Administration chapter.
2. Select *Restrict to Provision Guest Accounts*.
3. In *Guest Groups*, add the guest groups that this administrator manages.

Creating guest user groups

The guest group configuration determines the fields that are provided when you create a guest user account.

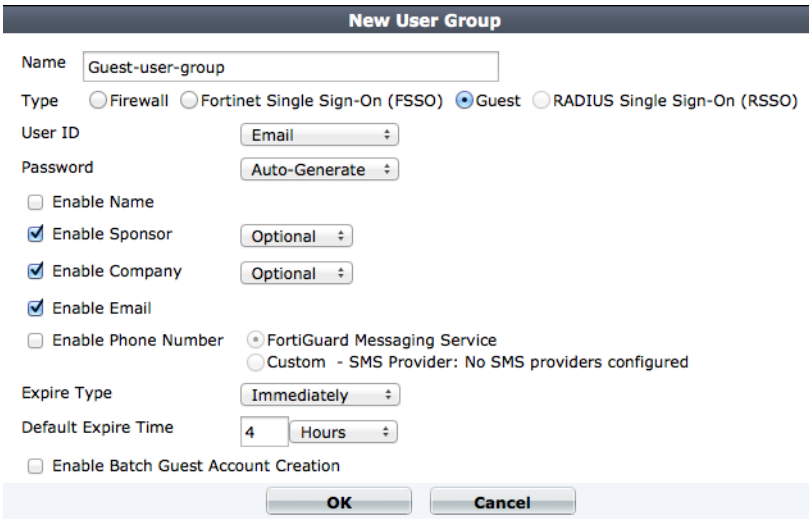
To create a guest user group

1. Go to *User & Device* > *User* > *User Group* and select *Create New*.
2. Configure the guest user group:

Name	Enter a name for the group.
Type	Guest
User ID	Select one of: • Email — User's email address • Specify — Administrator assigns user ID • Auto-Generate — FortiGate unit creates a random user ID
Password	Select one of: • Specify — Administrator assigns user ID • Auto-Generate — FortiGate unit creates a random password • Disable — no password
Enable Name	If enabled, user must provide a name.
Enable Sponsor	If enabled, user form has Sponsor field. Select *Required* or *Optional*.
Enable Company	If enabled, user form has Company field. Select *Required* or *Optional*.
Enable Email	If enabled, user is notified by email.
Enable Phone Number	If enabled, user is notified by SMS. Select whether FortiGuard Messaging Service or a another SMS provider is used. You can add SMS providers in *System* > *Config* > *Messaging Servers*.
Expire Type	Choose one of: Immediately —expiry time is counted from creation of account After first login — expiry time is counted from user's first login

Default Expire Time	Set the expire time. The administrator can change this for individual users.
Enable Batch Guest Account Creation	Create multiple accounts automatically. When this is enabled: • *User ID* and *Password* are set to *Auto-Generate*. • The user accounts have only *User ID, Password*, and *Expiration* fields. Only the *Expiration* field is editable. If the expiry time is a duration, such as “8 hours”, this is the time after first login. • You can print the account information. Users do not receive email or SMS notification.

Figure 45: Adding a Guest user group



Creating guest user accounts

Guest user accounts are not the same as local user accounts created in *User & Device* > *User* > *User Definition*. Guest accounts are not permanent; they expire after a defined time period. You create guest accounts in *User & Device* > *User* > *Guest Management*.

To create a guest user account

1. Go to *User & Device* > *User* > *Guest Management.*
2. In *Guest Groups*, select the guest group to manage.
3. Select *Create New* and fill in the fields in the *New User* form.

   Fields marked Optional can be left blank. The guest group configuration determines the fields that are available.
4. Select *OK*.
5. Select to print the temporary user account information or to email it to the email address of the account.
6. Select *Return*.

Guest Management Account List

Go to *User & Device* > *User* > *Guest Management* to create, view, edit or delete guest user accounts.

Create New	Creates a new guest user account.
Edit	Edit the selected guest user account.
Delete	Delete the selected guest user account.
Purge	Remove all accounts from the list.
Print	Print all of the user accounts in the group. You can print one or 3 accounts per page.
Send	Send the user account information to the guest. Depending on the group settings and user information, the information can be sent to the user by email or SMS.
Refresh	Update the list.
Guest Groups	Select the guest group to list. New accounts are added to this group.
User ID	The user ID. Depending on the guest group settings, this can be the user's email address, an ID that the administrator specified, or a randomly-generated ID.
Expires	Indicates a duration such as "3 hours". A duration on its own is relative to the present time. Or, the duration is listed as "after first login."

Batch guest account creation

You can use the guest user group auto generate options and guest user management options to quickly create any number of guest user accounts in just a few steps. Use the following steps to create 50 users with randomly generated usernames and passwords.

1. Go to *User & Device* > *User* > *User Groups* and select *Create New* to add a new user group.
2. Give the group a name, and set *Type* to *Guest*.
3. Select *Enable Batch Guest Account Creation* and select *OK*.
4. Go to *User & Device* > *User* > *Guest Management* and in the *Guest Groups* field select the guest user group that you just created.
5. *Select Create New* > *Multiple Users.*
6. Set the number of accounts to 50, set the expiry date, and select *OK*.

You can edit the individual accounts after they are created to send them to the user. You can also change the user name, password, and expiration time.

Vulnerability Scanning

The network vulnerability scanner helps you to protect your network assets (servers and workstations) by scanning them for security weaknesses. Configuration and operation of the vulnerability scanner has been simplified and the feature has been moved to *User & Device* > *Vulnerability Scan*.

This section describes how to configure a single FortiGate unit for network scanning and how to view the results of the scan.

Running and configuring scans and viewing scan results

You can configure regular network scans on a daily, weekly, or monthly basis.

To run a vulnerability scan

1. Go to *User & Device* > *Vulnerability Scan* > *Scan Definition* and select *Start Scan*.

   The vulnerability starts a scan using the current scanner settings. When the scan is running you can pause or stop it at any time. You can also watch the progress of the scan.
2. When the scan is complete go to *User & Device* > *Vulnerability Scan* > *Vulnerability Result* to view the results of the scan.

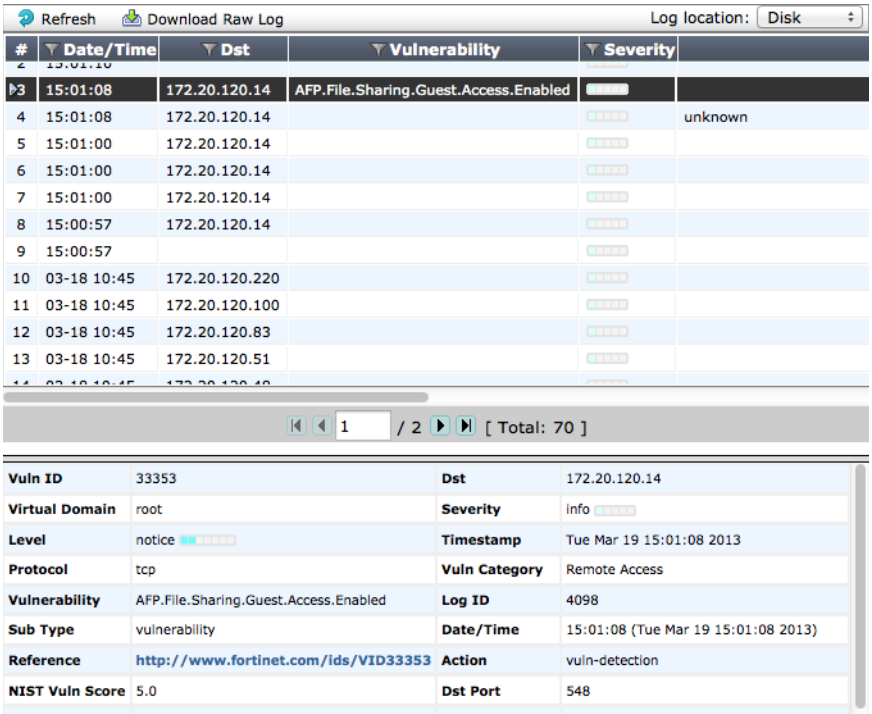
To run a vulnerability scan of one device or selected devices

1. Go to *User & Device* > *Vulnerability Scan* > *Scan Definition*.
2. Select the devices to scan from the *Asset Definitions* list.

   You can shift-click to select more than one device.
3. Select *Start*.

   The vulnerability starts a scan of the selected devices using the current scanner settings. When the scan is running you can pause or stop it at any time. You can also watch the progress of the scan.
4. When the scan is complete go to *User & Device* > *Vulnerability Scan* > *Vulnerability Result* to view the results of the scan. Select any log entry to view log details.

Figure 46: Example vulnerability scan results



To configure scanning

1. Go to *User & Device* > *Vulnerability Scan* > *Scan Definition*.

2. Beside *Schedule* select *Change* to set the scan schedule and mode:

Recurrence	Select *Daily*, *Weekly*, or *Monthly* and configure the details for the option you have selected.
Suspend Scan between	Set a time during which the scan should be paused if its running.
Vulnerability Scan Mode	**Quick** — check only the most commonly used ports **Standard** — check the ports used by most known applications **Full** — check all TCP and UDP ports

3. Select *Apply* to save the schedule and scan type.
4. Select *Create New* under *Asset Definitions* to select the devices on the network to scan.
5. Enter the following information and select *OK*:

Name	Enter a name for this asset.
Type	Select *IP Address* to add a single IP address. Select *Range* to add a range of IP addresses to scan.
IP Address	Enter the IP address of the asset. (*Type* is *IP Address*.)
Range	Enter the start and end of the IP address range. (*Type* is *Range*.)
Enable Scheduled Vulnerability Scanning	Select to allow this asset to be scanned according to the schedule. Otherwise the asset is not scanned during a scheduled vulnerability scan.
Windows Authentication	Select to use authentication on a Windows operating system. Enter the username and password in the fields provided.
Unix Authentication	Select to use authentication on a Unix operating system. Enter the username and password in the fields provided.

6. Select *Apply* to save the configuration.

FortiOS and BYOD

FortiOS can control network access for different types of personal mobile devices that your employees bring onto your premises. This is done by:

- Identifying and monitoring the types of devices connecting to your networks, wireless or wired
- Using MAC address based access control to allow or deny individual devices
- Creating policies based on device type
- Enforcing endpoint control on devices that can run FortiClient Endpoint Control software

This section describes:

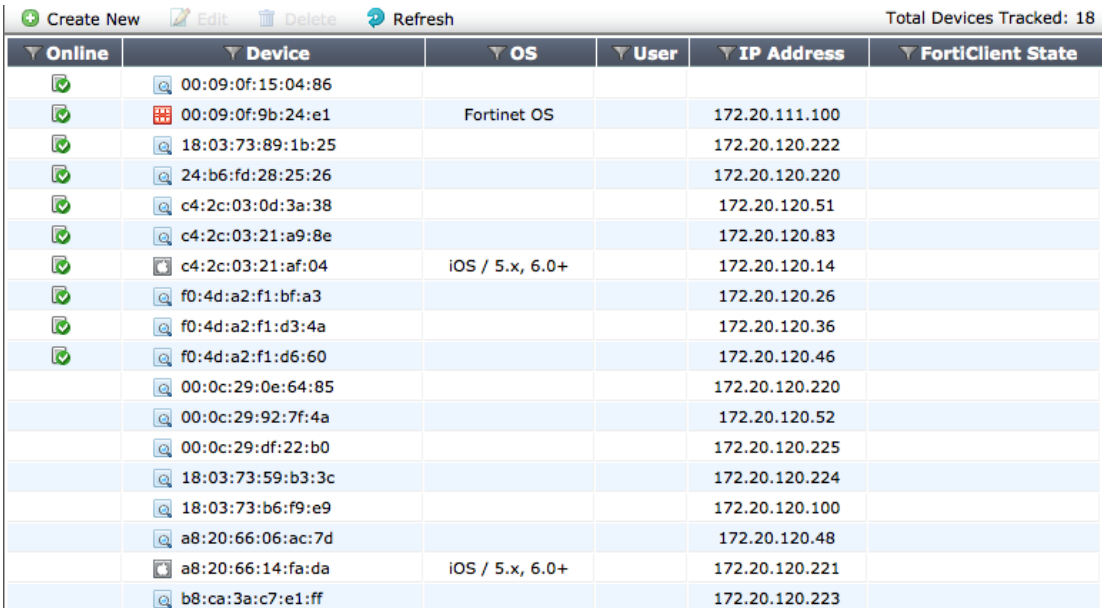
Device monitoring

The FortiGate unit can monitor your networks and gather information about the devices operating on those networks. Collected information includes:

- Whether the device is currently online
- MAC address
- IP address
- Operating system
- Hostname
- User
- How long ago the device was detected and on which FortiGate interface
- Whether FortiClient is installed on the device

You can go to *User & Device* > *Device* > *Device Definitions* to view this information.

Figure 47: The Device List



Online	Device	OS	User	IP Address	FortiClient State
✓	00:09:0f:15:04:86				
✓	00:09:0f:9b:24:e1	Fortinet OS		172.20.111.100	
✓	18:03:73:89:1b:25			172.20.120.222	
✓	24:b6:fd:28:25:26			172.20.120.220	
✓	c4:2c:03:0d:3a:38			172.20.120.51	
✓	c4:2c:03:21:a9:8e			172.20.120.83	
✓	c4:2c:03:21:af:04	iOS / 5.x, 6.0+		172.20.120.14	
✓	f0:4d:a2:f1:bf:a3			172.20.120.26	
✓	f0:4d:a2:f1:d3:4a			172.20.120.36	
✓	f0:4d:a2:f1:d6:60			172.20.120.46	
	00:0c:29:0e:64:85			172.20.120.220	
	00:0c:29:92:7f:4a			172.20.120.52	
	00:0c:29:df:22:b0			172.20.120.225	
	18:03:73:59:b3:3c			172.20.120.224	
	18:03:73:b6:f9:e9			172.20.120.100	
	a8:20:66:06:ac:7d			172.20.120.48	
	a8:20:66:14:fa:da	iOS / 5.x, 6.0+		172.20.120.221	
	b8:ca:3a:c7:e1:ff			172.20.120.223	

Device monitoring is enabled separately on each interface.

To configure device monitoring

1. Go to *System* > *Network* > *Interfaces* and edit a FortiGate interface to use for device monitoring.
2. Under *Device Management* select *Detect and Identify Devices*.
3. If you plan to use the Vulnerability scanner to scan discovered devices for vulnerabilities, select *Add New Devices to Vulnerability Scan List.*
4. Select *OK*.
5. Repeat for all interfaces to use for device monitoring.

To edit device information

1. Go to *User & Device* > *Device* > *Device Definitions* and double-click the entry to edit it.
2. Enter an *Alias* to identify the device.

   This is step is compulsory. The alias replaces the MAC address in the device list.
3. If the device can have more than on MAC address, add them to the device.
4. Optionally add the device to a custom device group.
5. Change other information as needed.
6. Select *OK*.

To add a device manually

1. Go to *User & Device* > *Device* > *Device Definitions* and select *Create New*.
2. Enter the following information.
   - Alias (required)
   - MAC address
   - Device Type
3. Optionally, add additional MAC addresses, select a *Custom Group* and enter *Comments*.
4. Select *OK*.

Device Groups

Device Groups are used in device policies to specify which devices match the policy. FortiOS automatically adds detected devices of well-known device types to predefined device groups. You can also create custom device groups so that you can create a different policy for specific, known devices.

Table 2: Predefined Device Groups

	Devices
Android Phone	Android-based phones.
Android Tablet	Android-based Tablets.
BlackBerry Phone	BlackBerry-based phones.
BlackBerry Playbook	BlackBerry-based tablets.
Collected Emails	All devices from which FortiOS has collected a user email address.
Fortinet Device	FortiGate, FortiManager, FortiAnalyzer, FortiMail, etc.
Gaming Console	All Gaming consoles listed in the Device Visibility database. This includes Xbox, PS2, PS3, Wii, PSP.
iPad	IOS-based tablets.
iPhone	IOS-based phones.
IP Phone	IP phones.
Linux PC	Linux-based PCs.
Mac	Apple Macintosh computers.
Media Streaming	Media streaming devices such as Apple TV.
Router/NAT Device	Routers and other gateway devices.
Windows Phone	Windows OS based phones.
Windows PC	Windows-based PCs.
Windows Tablet	Windows-based tablets.
Other Network Device	All other network devices not categorized under any other group.
All	All devices.

Creating a custom device group

The predefined device groups are automatically populated. When you create a custom device group, you choose the members. Adding a device that the FortiGate unit has already detected is easiest. But you can also add a device that has not yet been detected if you know its MAC address.

To create the custom device group

1. Go to *User & Device* > *Device* > *Device Groups* and select *Create New*.

2. Enter a name for the group.
3. Add devices to the group.
4. Select *OK*.

Controlling access with a MAC Address Access Control List

A MAC Address Access Control List is best used to handle exceptions. If you want to limit network access to a larger group, such as your employees, it is better to create a custom device group and specify that group in your device-based security policies.

A MAC Address Access Control List functions as either a list of blocked devices or a list of allowed devices. This is determined by the *Unknown MAC Address* entry.

- By default, unknown MAC addresses are allowed: *Action* is *Assign IP*. You add an entry for each MAC address that you want to block and set its *Action* to *Block*.
- If you want to restrict access to a limited set of devices, you set the *Unknown MAC Address* entry to *Block* and add an entry for each allowed MAC address with *Action* set to *Assign IP.*

To create a MAC Address Access Control List

1. In the SSID or other interface configuration, select *Enable DHCP Server*.
2. Enter the required *Address Range* and *Netmask*.
3. Expand *MAC Address Access Control List*.
4. Select *Create New* and enter the device's *MAC Address*.
5. Select *Assign IP* to allow the device or *Block* to block the device and then select *OK*.
6. Repeat Steps 4 and 5 for each additional MAC address entry.

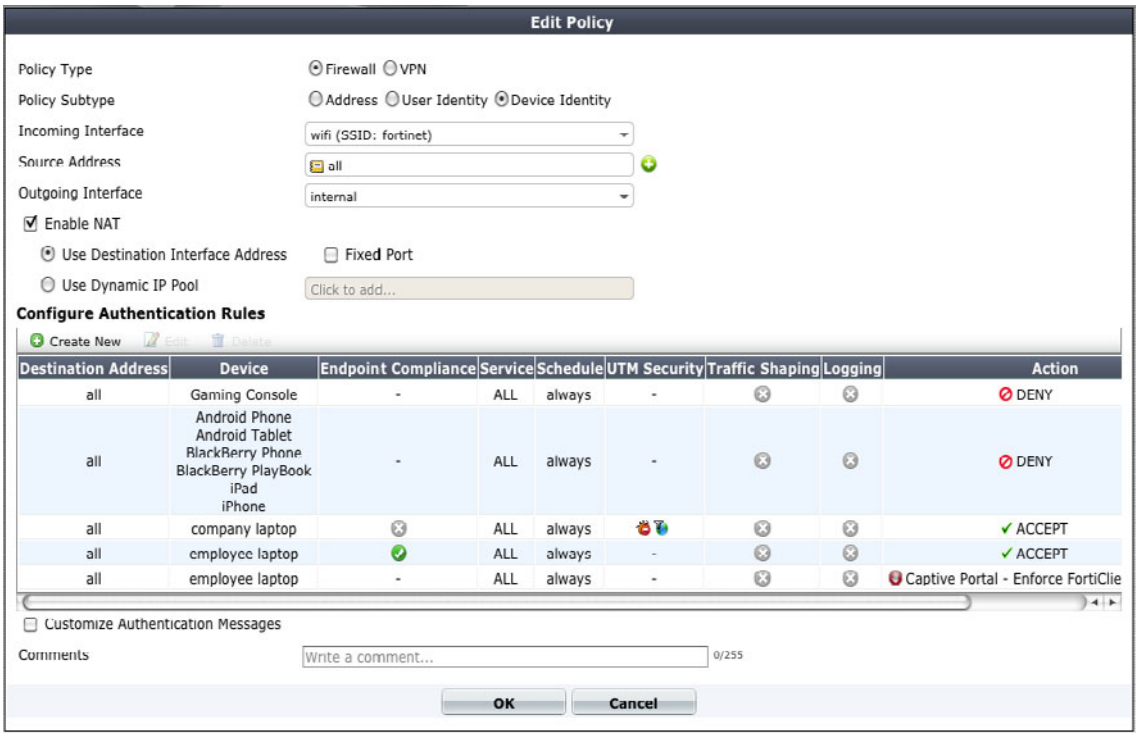
Device policies

Policies based on device identity enable you to implement policies according to device type. For example:

- Gaming consoles cannot connect to the company network or the Internet.
- Personal tablet and phone devices can connect to the Internet but not to company servers.
- Company-issued laptop computers can connect to the Internet and company servers. Web filtering and antivirus are applied.
- Employee laptop computers can connect to the Internet, but web filtering is applied. They can also connect to company networks, but only if FortiClient Endpoint Security is installed to protect against viruses.

Figure 48 shows these policies implemented for WiFi to the company network.

Figure 48: Device policies for WiFi access to the company network



Device-based security policies are similar to policies based on user identity:

- The policy enables traffic to flow from one network interface to another.
- NAT can be enabled.
- Authentication rules can allow or deny specific devices or device groups.
- UTM protection can be applied.

To create a device identity policy

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. In *Policy Subtype*, select *Device Identity*.
3. Choose *Incoming Interface*, *Source Address*, and *Outgoing Interface* as you would for any security policy.
4. Select *Enable NAT* if appropriate.

   You are now ready to create authentication rules.

To create an authentication rule

1. Select *Create New.*
2. Enter *Destination*, *Schedule*, and *Service* as you would for any security policy.
3. In *Device*, select the devices or device groups to which this policy applies.

   You can select multiple devices or groups.
4. Select *Compliant with Endpoint Profile* if you want to enforce use of FortiClient Endpoint Security by the client devices. This is available here only if Action is ACCEPT. See “Adding endpoint control” next.
5. Select one of the following for Action:
   - ACCEPT
   - DENY

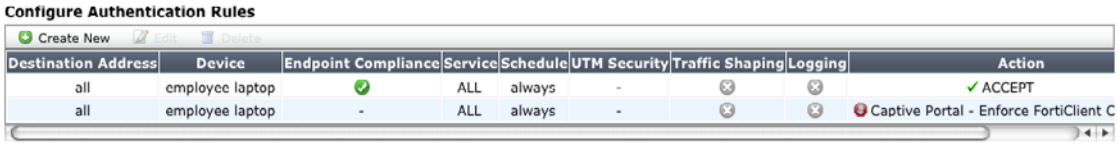
6. Configure *UTM Security Profiles* as you would for any security policy.
7. Select *OK*.
8. Select *OK* again to complete creation of the security policy.

Adding endpoint control

Optionally, you can require that user's devices have FortiClient Endpoint Security software installed. The software provides FortiOS more detailed information about the applications being used. FortiOS pushes its endpoint profile to the FortiClient software, configuring network protection such as antivirus, application control, and web category filtering. Devices without an up-to-date installation of FortiClient software are restricted to a captive portal that provides links from which the user can download a FortiClient installer.

If you have already created an ACCEPT rule for particular device groups, you simply edit this rule and enable *Compliant with Endpoint Profile*. Then you add a second rule that sends the same devices to the Enforce FortiClient Compliance captive portal. Devices lacking the required FortiClient software arrive at this policy because they do not match the preceding policy.

Figure 49: Endpoint compliance rule and captive portal rule



Device policy portal options

The following portal options are available when configuring a device policy:

- Attempt to detect all Unknown device types before implicit deny
- Redirect all non-compliant/unregistered FortiClient compatible devices to a captive portal

  Custom portals are available for Windows, Mac OS, iPhone/iPad and Android devices. These portals acts as a quarantine for devices that are not protected by FortiClient Endpoint Security. The portal provides links to obtain the FortiClient software. The user can retry connecting after installing the FortiClient software.
- Prompt E-mail Collection Portal for all devices

  This portal is used to collect an email address as a means of identifying the device user. When the email address has been verified, the device is added to the Collected Emails device group.

Creating the WiFi SSID

In order to create a WiFi SSID using the web-based manager, the WiFi Controller (called WiFi & Switch Controller on FortiGate models 100D, 200D, 240D, 600C, 800C, and 1000C) feature must be enabled using Feature Select. For more information, see "Feature Select" on page 168.

Both guest and employee devices will need an SSID (WiFi network) with open security. This means that no passphrase is required to join the SSID. Device policies will determine who gets access to network resources. By default, open security is not available in the WiFi SSID configuration.

To configure the SSID

1. Go to *WiFi Controller* > *WiFi Network* > *SSID* and select *Create New*.
2. Enter the following information and select OK:

Name	byod-example
IP/Netmask	10.10.110.1/24
Administrative Access	Ping (to assist with testing)
Enable DHCP Server	Enable
Address Range	10.10.110.2 - 10.10.110.199
Netmask	255.255.255.0
Default Gateway	Same As Interface IP
SSID	byod-guest
Security Mode	Open
Block Intra-SSID Traffic	Select.
Leave other settings at their default values.	

For detailed information about creating a WiFi SSID, see the Deploying Wireless Networks chapter of the FortiOS Handbook.

Configuring Internet access for guests with mobile devices

Guest devices have access only to the Internet. You need a device policy that allows traffic to flow from the WiFi SSID to the Internet interface. Within that policy, you need an authentication rules to allow access for the various types of devices.

To create the device policy

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Enter the following information:

Policy Type	Firewall
Policy Subtype	Device Identity
Incoming Interface	byod-example
Source Address	all
Outgoing Interface	wan1
Enable NAT	Enable.

You are now ready to create the authentication rule.

To create the authentication rule

1. In *Configure Authentication Rules*, select *Create New* and enter:

Destination Address	all
Device	Device or Device Group
Compliant with Endpoint Profile	not selected
Schedule	always
Service	ALL
Action	ACCEPT

2. Select *OK*.
3. If asked, confirm that you accept FortiOS will enable device identification on the source interface.

   The rule is now configured.
4. Select *OK* to complete configuration of the security policy.

Client Reputation

The Security scan types available on FortiGate units are varied and tailored to detect specific attacks. However, sometimes user/client behavior can increase the risk of attack or infection. For example, if one of your network clients receives email viruses on a daily basis while no other clients receive these attachments, extra measures may be required to protect the client, or a discussion with the user about this issue may be worthwhile.

Before you can decide on a course of action, you need to know the problem is occurring. Client reputation can provide this information by tracking client behavior and reporting on activities that you determine are risky or otherwise noteworthy.

Activities you can track include:

- Bad Connection Attempts: A typical BOT behavior is to connect to some hosts that do not exist on the Internet. This is because the BOT home needs to constantly change itself to dodge legislative enforcement or to hide from AV vendors. Bad connection attempts are tracked by:
  - Look ups for a DNS name that does not exist.
  - Connection attempts to an IP address that has no route.
  - HTTP 404 errors
- Packets that are blocked by security policies.
- Intrusion protection: Attack detected. The effect on reputation increases with severity of attack. A subscription to FortiGuard IPS updates is required.
- Malware protection: Malware detected. This requires a subscription to FortiGuard Antivirus updates.
- Web activity: Visit to web site in risky categories, including Potentially Liable, Adult/Mature Content, Bandwidth Consuming and Security Risk. A subscription to FortiGuard Web Filtering is required.
- Application protection: Client uses software in risky categories, including Botnet, P2P, Proxy, and Games applications. A subscription to FortiGuard IPS updates is required.
- Geographical locations that clients are communicating with. Access to the FortiGuard geographic database and a valid Fortinet support contract is required.

You can configure how severely each type of tracked activity will impact the reputation of the client in a sliding scale of Low, Medium, High or Critical. You can also choose to ignore an activity by setting it to Off. When an activity is turned off, it will have no effect on reputation.

You can enable client reputation tracking for your FortiGate unit by going to *Security Profiles* > *Client Reputation* > *Threat Level Definition*. Turning on client reputation tracking turns on traffic logging for all security policies, for all DoS policies and for all sniffer policies. While client reputation is enabled, logging cannot be turned off for these policies. Traffic logging must be enabled for data to be added to the client reputation database.

Client reputation only highlights risky activity and does not include tools to stop it. Instead, client reputation is a tool that exposes risky behavior. When you uncover risky behavior that you are concerned about, you can take additional action to stop it. That action could include adding more restrictive security policies to block the activity or increase UTM protection. You can also taking other measures outside your FortiGate unit to stop the activity.

To support client reputation your FortiGate unit must be registered, have a valid support contract and be licensed for FortiGuard antivirus, IPS and Web Filtering.

After client reputation is turned on, the FortiGate unit tracks recent behavior using a sliding window and displays current data for this window. The client reputation monitor displays clients and their activities in charts ordered according to how risky the behavior exhibited by the client is.

Client Reputation data is stored in traffic log messages in the newly added client reputation fields (crscore and craction). When you enable client reputation *Log UTM Events* or *Log all Sessions* is enabled in all security policies. *Log UTM Events* records traffic log messages for UTM sessions and *Log all Sessions* records traffic logs for all sessions. When Client Reputation is enabled you cannot select *No Log* in a security policy. Using client reputation data in log messages, you can configure FortiAnalyzer to produce a client reputation report.

Enabling client reputation can affect system performance if you had not been using traffic logging.

This chapter describes:

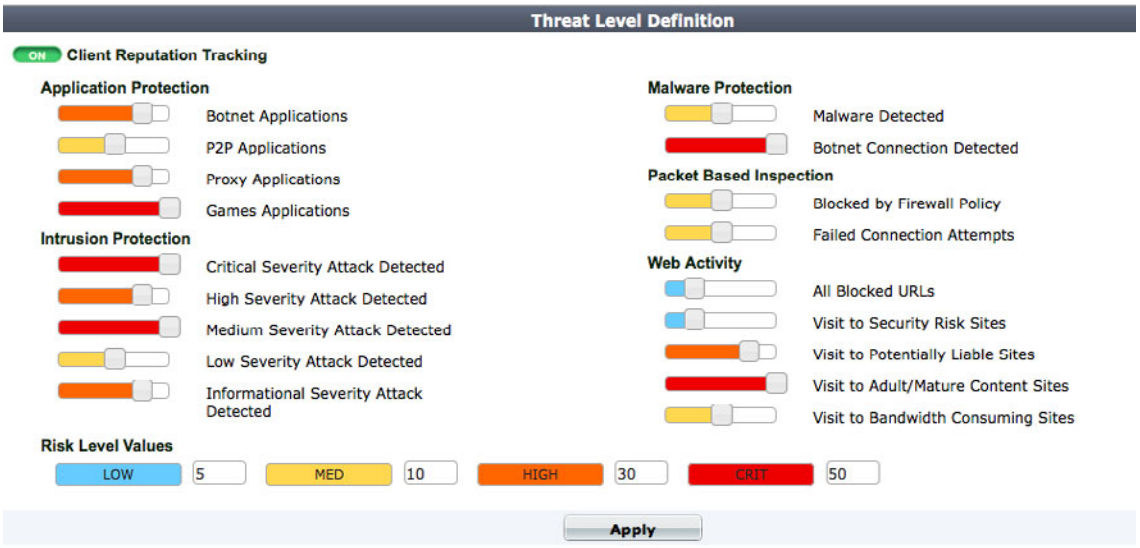
Setting the client reputation profile/definition

Configure the client reputation profile by going to *Security Profiles* > *Client Reputation* > *Threat Level Definition*. You configure one client reputation profile for all of the activity monitored by the FortiGate unit. The profile sets the risk levels for the types of behavior that client reputation monitors. You can set the risk to off, low, medium, high and critical for the following types of behavior:

- Application Protection
  - Botnet applications
  - P2P applications
  - Proxy applications
  - Games applications
- Intrusion protection (IPS)
  - Critical severity attack detected
  - High severity attack detected
  - Medium severity attack detected
  - Low severity attack detected
  - Informational severity attack detected
- Malware Protection
  - Malware detected
  - Botnet connection detected
- Packet based inspection
  - Blocked by firewall policy
  - Failed connection attempts

- Web Activity
  - All blocked URLs
  - Visit to security risk sites
  - Visit to potentially liable sites
  - Visit to adult/mature content sites
  - Visit to bandwidth consuming sites

Figure 50: Default client reputation profile



To configure the profile, decide how risky or dangerous each of the types of behavior are to your network and rate them accordingly. The higher you rate a type of behavior, the more visible clients engaging in this behavior will become in the client reputation monitor and the more easily you can detect this behavior.

For example, if you consider malware a high risk for your network, you can set the client reputation profile for malware to high or critical (as it is in the default client reputation profile). Then, whenever any amount of malware is detected, clients that originated the malware will be very visible in the client reputation monitor.

Set the risk to off for types of activity that you do not want client reputation to report on. This does not reduce the performance requirements or the amount of data gathered by client reputation, just the report output.

You can change a profile setting at any time and data that has already been collected will be used.

It is normally not necessary to change the *Risk Level Values* but it can be done if you need to alter the relative importance of the risk settings.

Applying client reputation monitoring to your network

Client reputation monitoring is applied to network traffic by going to *Security Profiles* > *Client Reputation* > *Threat Level Definition* turning on *Client Reputation Tracking* and selecting *Apply*.

You can then either change the client reputation profile used by your FortiGate unit or you can accept the default profile. The client reputation profile indicates how risky you consider different types of client behavior to be. See “Expanding client reputation to include more types of behavior” on page 109 for details.

Viewing client reputation results

Client reputation results can be viewed in the *Threat History* widget, which is found at *System* > *Dashboard* > *Threat History*.

The *Threat History* widget displays threat severity over time. Specific time periods can be selected, at which point drilldown menus are available to view more information about the threats, including information about threat types and the sources of each incident.

Figure 51: The *Threat History* widget

Expanding client reputation to include more types of behavior

You can use the following command to change the client reputation profile from the CLI to include client reputation reporting about more settings:

```
config client-reputation profile
```

In addition to the settings configurable from the web-based manager, you can also set the following options:

- `geolocation` to enable reporting on connections to and from different countries (geographical locations). For example, use the following command to indicate that you consider communication with Aruba to be medium risk:

```
config client-reputation profile
  config geolocation
    edit 0
      set country AW
      set level medium
    end
  end
```

- `url-block-detected` to report on connections blocked by web filtering. Use the following command to enable reporting about blocked URLs and set the risk level to medium:

```
config client-reputation profile
  set url-block-detected medium
end
```

From the CLI you can configure client reputation to report more FortiGuard web filtering categories and more types of applications. For example, to report on social network activity (application control category 23):

```
config client-reputation-profile
  config application
    edit 0
      set category 23
      set level medium
    end
  end
```

To report on the local web filtering category (category 22):

```
config client-reputation-profile
  config web
    edit 0
      set group 22
      set level medium
    end
  end
```

Client reputation execute commands

The `execute client-reputation` command includes the following options:

- `erase`, deletes all client reputation data.
- `host-count`, lists the clients that started sessions recorded by client reputation
- `host-detail`, for a specified client's IP address, displays the client reputation traffic log messages saved for that client.
- `host-summary`, for a specified client's IP address, displays the client's IP address, total entries, and total score.
- `purge`, deletes all data from the client reputation database.
- `topN`, display the top N clients identified by client reputation.

Client reputation diagnose commands

The `diagnose client-reputation` command includes the following options

- `convert-timestamp` convert a client reputation database timestamp to date and time
- `test-all` adds log messages from multiple sources to the client reputation database for testing
- `test-app` adds application control log messages to the client reputation database for testing
- `test-ips` adds Intrusion Protection log messages to the client reputation database for testing
- `test-webfilter` adds webfilter log messages to the client reputation database for testing

Wireless

New wireless features include:

- Wireless IDS
- WiFi performance improvements
- FortiAP web-based manager and CLI
- WiFi guest access provisioning
- FortiAP local bridging (Private Cloud-Managed AP)
- WiFi data channel encryption
- Wireless client load balancing for high-density deployments
- Bridge SSID to FortiGate wired network

Wireless IDS

FortiGate wireless IDS monitors wireless traffic for a wide range of security threats by detecting and reporting on possible intrusion attempts. When an attack is detected, the FortiGate unit records a log message.

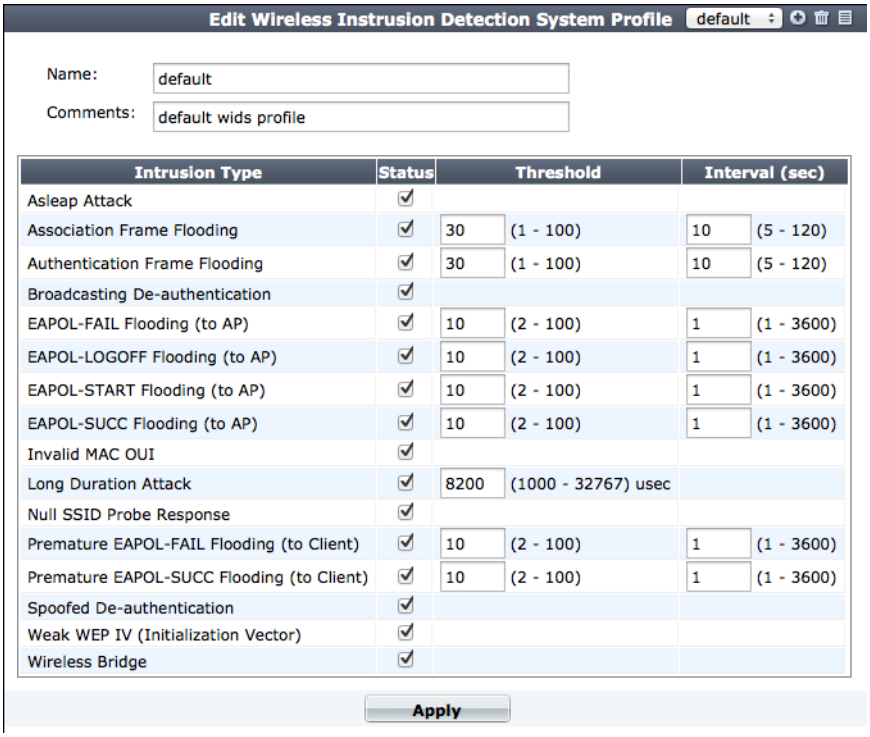
You can create a WIDS profile to enable the following types of intrusion detection among others:

- Unauthorized Device Detection
- Rogue/Interfering AP Detection
- Adhoc Network Detection and Containment
- Wireless Bridge Detection
- Misconfigured AP Detection
- Weak WEP Detection
- Multi Tenancy Protection
- MAC OUI Checking

You can enable wireless IDS by going to *WiFi Controller* > *WiFi Network* > *Custom AP Profiles* and editing an access point profile or creating a new one.

Inside the profile, set *WIDS Profile* to the name of a wireless IDS profile to apply wireless IDS protection to the access points that uses the profile. FortiGate units include a *default* wireless IDS profile. You can customize this profile or create additional profiles by going to WiFi *Controller* > *WiFi Network* > *WIDS Profiles.*

Figure 52: Configuring a WIDS profile



You can also use the `config wireless-controller wids-profile` command to configure Wireless Intrusion Detection (WIDS) profiles.

Syntax

```
config wireless-controller wids-profile
  edit <wids-profile_name>
    set comment <comment_str>
    set asleap-attack {enable | disable}
    set assoc-frame-flood {enable | disable}
    set auth-frame-flood {enable | disable}
    set deauth-broadcast {enable | disable}
    set eapol-fail-flood {enable | disable}
    set eapol-fail-intv <int>
    set eapol-fail-thres <int>
    set eapol-logoff-flood {enable | disable}
    set eapol-logoff-intv <int>
    set eapol-logoff-thres <int>
    set eapol-pre-fail-flood {enable | disable}
    set eapol-pre-fail-intv <int>
    set eapol-pre-fail-thres <int>
    set eapol-pre-succ-flood {enable | disable}
    set eapol-pre-succ-intv <int>
    set eapol-pre-succ-thres <int>
    set eapol-start-flood {enable | disable}
    set eapol-start-intv <int>
```

```
    set eapol-start-thres <int>
    set eapol-succ-flood {enable | disable}
    set eapol-succ-intv <int>
    set eapol-succ-thres <int>
    set invalid-mac-oui {enable | disable}
    set long-duration-attack {enable | disable}
    set long-duration-thresh <int>
    set null-ssid-probe-resp {enable | disable}
    set spoofed-deauth {enable | disable}
    set weak-wep-iv {enable | disable}
    set wireless-bridge {enable | disable}
end
```

Variable	Description	Default
`<wids-profile_name>`	Enter a name for this WIDS profile.	No default.
`comment <comment_str>`	Optionally, enter a descriptive comment.	No default.
`asleap-attack {enable | disable}`	Enable to detect asleap attack (attempt to crack LEAP security).	disable
`assoc-frame-flood {enable | disable}`	Enable to detect association frame flood attack.	disable
`auth-frame-flood {enable | disable}`	Enable to detect authentication frame flood attack.	disable
`deauth-broadcast {enable | disable}`	Enable to detect deauthentication broadcasts which can disrupt wireless services to multiple clients.	disable
`eapol-fail-flood {enable | disable}`	Enable to detect EAP FAIL flood attack.	disable
`eapol-fail-intv <int>`	Set EAP FAIL detection interval.	1
`eapol-fail-thres <int>`	Set EAP FAIL detection threshold.	10
`eapol-logoff-flood {enable | disable}`	Enable to detect EAP LOGOFF flood attack.	disable
`eapol-logoff-intv <int>`	Set EAP LOGOFF detection interval.	1
`eapol-logoff-thres <int>`	Set EAP LOGOFF detection threshold.	10
`eapol-pre-fail-flood {enable | disable}`	Enable to detect EAP premature FAIL flood attack.	disable
`eapol-pre-fail-intv <int>`	Set EAP premature FAIL detection interval.	1
`eapol-pre-fail-thres <int>`	Set EAP premature FAIL detection threshold.	10
`eapol-pre-succ-flood {enable | disable}`	Enable to detect EAP premature SUCC flood attack.	disable
`eapol-pre-succ-intv <int>`	Set EAP premature SUCC detection interval.	1
`eapol-pre-succ-thres <int>`	Set EAP premature SUCC detection threshold.	10

Variable	Description	Default
`eapol-start-flood {enable | disable}`	Enable to detect EAP START flood attack.	disable
`eapol-start-intv <int>`	Set EAP START detection interval.	1
`eapol-start-thres <int>`	Set EAP START detection threshold.	10
`eapol-succ-flood {enable | disable}`	Enable to detect EAP SUCC flood attack.	disable
`eapol-succ-intv <int>`	Set EAP SUCC detection interval.	1
`eapol-succ-thres <int>`	Set EAP SUCC detection threshold.	10
`invalid-mac-oui {enable | disable}`	Enable to detect use of spoofed MAC addresses. (The first three bytes should indicate a known manufacturer.)	disable
`long-duration-attack {enable | disable}`	Enable for long duration attack detection based on long-duration-thresh.	disable
`long-duration-thresh <int>`	Enter the duration in usec for long-duration attack detection. This is available when long-duration-attack is enable.	8200
`null-ssid-probe-resp {enable | disable}`	Detect attacks that include an incorrectly formed response packets that include a null SSID. This attack can cause wireless clients to crash.	disable
`spoofed-deauth {enable | disable}`	Enable to detect spoofed deathentication packets.	disable
`weak-wep-iv {enable | disable}`	Enable to detect APs using weak WEP encryption.	disable
`wireless-bridge {enable | disable}`	Enable to detect wireless bridge operation, which is suspicious if your network doesn't use a wireless bridge.	disable

WiFi performance improvements

FortiOS 5.0 improves performance for WiFi users connecting to the wifi network on a FortiWiFi unit or remotely on FortiAP units. WiFi traffic is now handled in the FortiOS kernel like other network traffic, rather than in a separate application.

FortiAP web-based manager and CLI

You can now log into a FortiAP web-based manager to view FortiAP status as well as view and change the FortiAP configuration. Logging into the FortiAP web-based manager is similar to logging into the FortiGate web-based manager.

The FortiAP CLI now includes more configuration commands and a complete set of diagnose commands.

Configuration commands include the following

`cfg -h`	Display help for all commands.
`cfg -r var`	Remove variables.
`cfg -e`	Export variables.
`cfg -s`	List variables.
`cfg -x`	Reset to factory defaults.
`cfg -c`	Commit the change to flash.
`cfg -a var=value`	Add or change variables.

Diagnose commands include:

`cw_diag help`	Display help for all diagnose commands.
`cw_diag uptime`	Show daemon uptime.
`cw_diag --tlog <on|off>`	Turn on/off telnet log message.
`cw_diag --clog <on|off>`	Turn on/off console log message.
`cw_diag baudrate [9600 | 19200 | 38400 | 57600 | 115200]`	Set the console baud rate.
`cw_diag plain-ctl [0|1]`	Show or change current plain control setting.
`cw_diag sniff-cfg ip port`	Set sniff server ip and port.
`cw_diag sniff [0|1|2]`	Enable/disable sniff packet.
`cw_diag stats wl_intf`	Show wl_intf status.
`cw_diag admin-timeout [30]`	Set shell idle timeout in minutes.
`cw_diag -c wtp-cfg`	Show current wtp config parameters in control plane.
`cw_diag -c radio-cfg`	Show current radio config parameters in control plane.
`cw_diag -c vap-cfg`	Show current vaps in control plane.
`cw_diag -c ap-rogue`	Show rogue APs pushed by AC for on-wire scan.
`cw_diag -c sta-rogue`	Show rogue STAs pushed by AC for on-wire scan.
`cw_diag -c arp-req`	Show scanned arp requests.
`cw_diag -c ap-scan`	Show scanned APs.
`cw_diag -c sta-scan`	Show scanned STAs.
`cw_diag -c sta-cap`	Show scanned STA capabilities.
`cw_diag -c wids`	Show scanned WIDS detections.

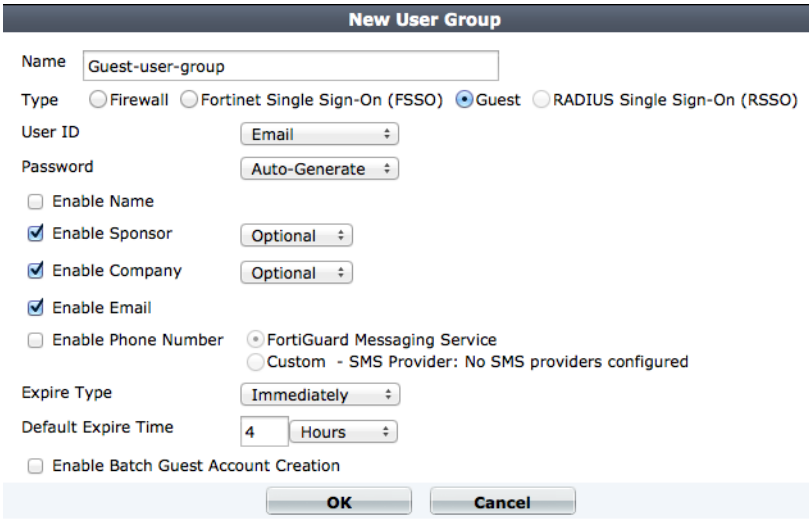
`cw_diag -c darrp`	Show darrp radio channel.
`cw_diag -c mesh`	Show mesh status.
`cw_diag -c mesh-veth-acinfo`	Show mesh veth ac info, and mesh ether type.
`cw_diag -c mesh-veth-vap`	Show mesh veth vap.
`cw_diag -c mesh-veth-host`	Show mesh veth host.
`cw_diag -c mesh-ap`	Show mesh ap candidates.
`cw_diag -c scan-clr-all`	Flush all scanned AP/STA/ARPs.
`cw_diag -c ap-suppress`	Show suppressed APs.
`cw_diag -c sta-deauth`	Ee-authenticate an STA.

WiFi guest access provisioning

Guest access provisioning allows you to easily add guest accounts to your FortiGate unit. These accounts are mainly used to authenticate guest WiFi users for temporary access to a WiFi network managed by a FortiGate unit.

Guest access configuration begins by going to *User & Device* > *User Definition* > *User Group* and adding one or more guest user groups.

Figure 53: Adding a Guest user group



Many guest account options are available including:

- Email address or user name to identify the guest account
- Requiring a password or no password to log in
- Require a sponsor or company name
- Sending the user's account information to them using email, FortiGuard Messaging Service, or SMS messages
- Configurable account expiry time, starting immediately or after the first login
- Batch guest account creation using auto-generated user IDs and passwords

Guest users are added, removed and managed from *User & Device* > *User* > *Guest Management*. From this page, you select the guest user group to change, then add users to it, edit users that have been added or purge all users. When you add the user, you can customize the account expiration date and time.

To provide guest users with their account information, you can select the account from this Guest Management page and select *Send* to print the guest account credentials or send them to the user as an email or SMS message.

Adding guest access to a WiFi network

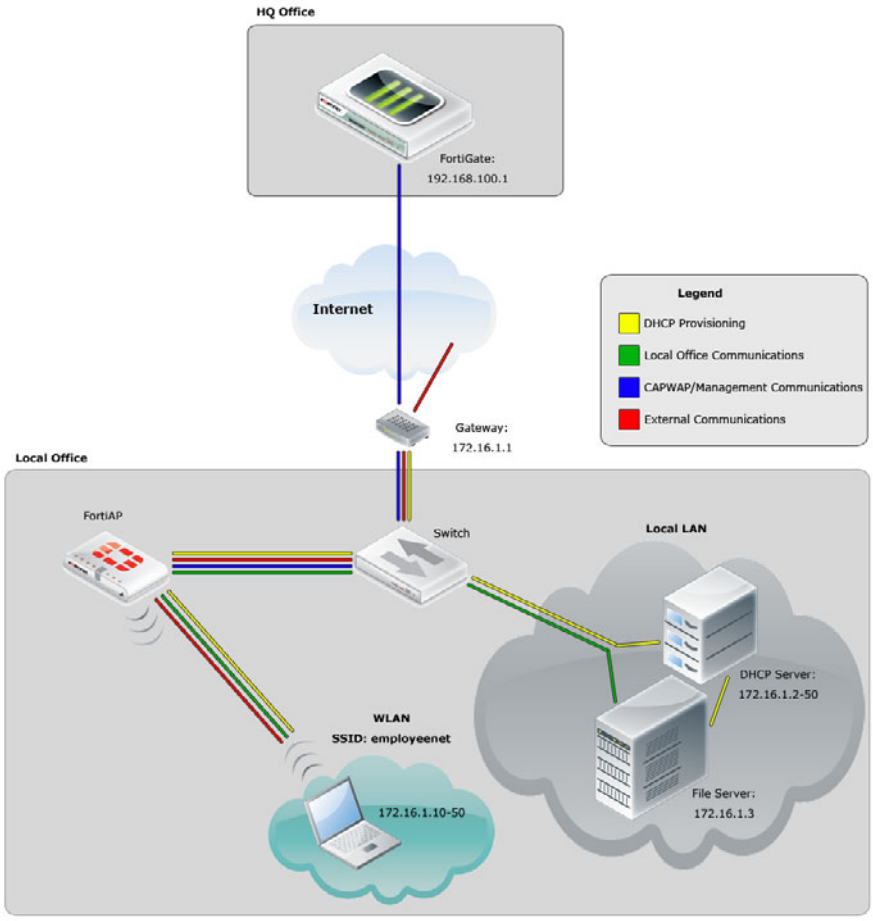
To apply guest access provisioning to a Wifi network, set the *Security Mode* of an SSID to *Captive Portal* and select one or more guest user groups. Guest users can then log into the portal using their guest account.

FortiAP local bridging (Private Cloud-Managed AP)

A FortiAP unit can provide WiFi access to a LAN, even when the wireless controller is located remotely. This configuration is useful for the following situations:

- Installations where the WiFi controller is remote and most of the traffic is local or uses the local Internet gateway
- Wireless-PCI compliance with remote WiFi controller
- Telecommuting, where the FortiAP unit has the WiFi controller IP address pre-configured and broadcasts the office SSID in the user's home or hotel room. In this case, data is sent in the wireless tunnel across the Internet to the office and should have encryption using DTLS enabled.

Figure 54: Remotely-managed FortiAP providing WiFi access to local network



On the remote FortiGate wireless controller, the WiFi SSID is created with the *Traffic Mode* set to *Local Bridge with FortiAP's Interface*. In this mode, no IP addresses are configured. The FortiAP unit's WiFi and Ethernet interfaces behave like a switch. WiFi client devices obtain IP addresses from the same DHCP server as wired devices on the LAN.

There can be only one Bridge mode SSID per FortiAP unit. The Local Bridge feature cannot be used in conjunction with Wireless Mesh features.

To configure a FortiAP local bridge - web-based manager

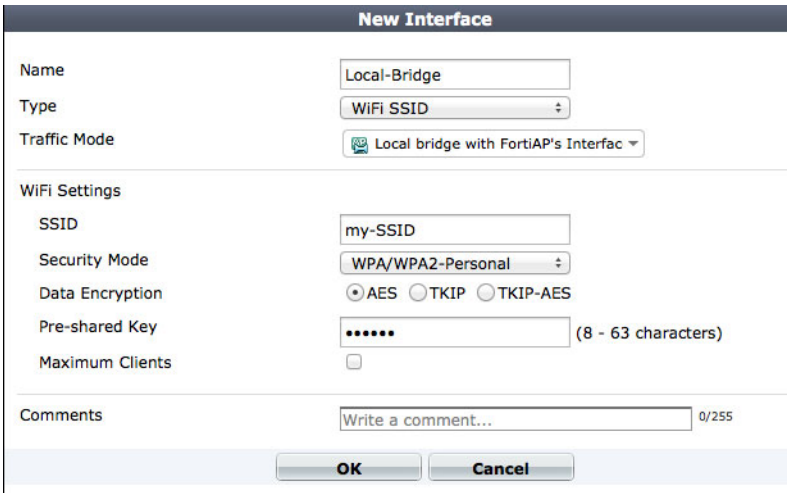
1. Go to *WiFi Controller* > *WiFi Network* > *SSID* and select *Create New*.
2. Enter:

Interface name	A name for the new WiFi interface.
Traffic Mode	Local bridge with FortiAP's Interface

SSID	The SSID visible to users.
Security Mode **Data Encryption** **Preshared Key**	Configure security as you would for a regular WiFi network.

3. Select OK.
4. Go to *WiFi Controller* > *Managed Access Points* > *Managed FortiAP,* select the FortiAP unit for editing.
5. Authorize the FortiAP unit.
6. The FortiAP unit can carry regular SSIDs in addition to the Bridge SSID.

Figure 55:SSID configured for Local Bridge operation



To configure a FortiAP local bridge - CLI

This example creates a WiFi interface “branchbridge” with SSID “LANbridge” using WPA-Personal security, passphrase “Fortinet1”.

```
config wireless-controller vap
  edit "branchbridge"
    set vdom "root"
    set ssid "LANbridge"
    set local-bridging enable
    set security wpa-personal
    set passphrase "Fortinet1"
  end
config wireless-controller wtp
  edit FAP22B3U11005354
    set admin enable
    set vaps "branchbridge"
  end
```

WiFi data channel encryption

You can enhance the security of communication between a FortiGate wireless controller and a FortiAP unit by applying DTLS encryption to the data channel.

There are data channel encryption settings on both the FortiGate unit and the FortiAP unit. At both ends, you can enable Clear Text, DTLS encryption or both. The settings must agree or the FortiAP unit will not be able to join the WiFi network. By default, both Clear Text and DTLS-encrypted communication are enabled on the FortiAP unit, allowing the FortiGate setting to determine whether data channel encryption is used. If the FortiGate unit also enables both Clear Text and DTLS, Clear Text is used.

Data channel encryption settings are located in the Custom AP profile. If you use Automatic profile, only Clear Text is supported.

Data channel encryption is software-based and can affect performance. Verify that the system meets your performance requirements with encryption enabled.

Configuring DTLS on the FortiGate unit

To enable DTLS for the FAP320B-default profile, enter:

```
config wireless-controller wtp-profile
  edit FAP320B-default
    set dtls-policy dtls-enabled
  end
```

Configuring encryption on the FortiAP unit

The FortiAP unit has its own settings for data channel encryption.

Enabling CAPWAP encryption - FortiAP web-based manager

1 On the *System Information* page, in *WTP Configuration* > *AC Data Channel Security*, select one of:
- Clear Text
- DTLS Enabled
- Clear Text or DTLS Enabled (default)

2 Select *Apply*.

Enabling encryption - FortiAP CLI

You can set the data channel encryption using the AC_DATA_CHAN_SEC variable:

- 0 is Clear Text
- 1 is DTLS Enabled
- 2 is Clear Text or DTLS Enabled (default)

For example, to set security to DTLS and then save the setting, enter

```
cfg -a AC_DATA_CHAN_SEC=1
cfg -c
```

Wireless client load balancing for high-density deployments

Wireless load balancing allows your wireless network to distribute wireless traffic more efficiently among wireless access points and available frequency bands. FortiGate wireless controllers support the following types of client load balancing:

- Access Point Hand-off - the wireless controller signals a client to switch to another access point.
- Frequency Hand-off - the wireless controller monitors the usage of 2.4GHz and 5GHz bands, and signals clients to switch to the lesser-used frequency.

Load balancing is not applied to roaming clients.

Access point hand-off

Access point handoff wireless load balancing involves the following:

- If the load on an access point (ap1) exceeds a threshold (for example, 30 clients) then the client with the weakest signal will be signaled by the wireless controller to drop off and join another nearby access point (ap2).
- When one or more access points are overloaded (more than 30 clients) and a new client attempts to join a wireless network, the wireless controller selects the least busy access point that is closest to the new client and this access point is the one that responds to the client and the one that the client joins.

Frequency hand-off or band-steering

Encouraging clients to use the 5GHz WiFi band if possible enables those clients to benefit from faster interference-free 5GHz communication. The remaining 2.4GHz clients benefit from reduced interference.

The WiFi controller probes clients to determine their WiFi band capability. It also records the RSSI (signal strength) for each client on each band.

If a new client attempts to join the network, the controller looks up that client's MAC address in its wireless device table and determines if it's a dual band device. If it is not a dual band device, then its allowed to join. If it is a dual band device, then its RSSI on 5GHz is used to determine whether the device is close enough to an access point to benefit from movement to 5GHz frequency.

If both conditions of 1) dual band device and 2) RSSI value is strong, then the wireless controller does not reply to the join request of the client. This forces the client to retry a few more times and then timeout and attempt to join the same SSID on 5GHz. Once the controller see this new request on 5GHz, the RSSI is again measured and the client is allowed to join. If the RSSI is below threshold, then the device table is updated and the controller forces the client to timeout again. A client's second attempt to connect on 2.4GHz will be accepted.

Configuration

From the web-based manager, edit a custom AP profile and select *Frequency Handoff* and *AP Handoff* as required for each radio on the AP.

From the CLI, you configure wireless client load balancing thresholds for each custom AP profile. Enable access point hand-off and frequency hand-off separately for each radio in the custom AP profile.

```
config wireless-controller wtp-profile
  edit new-ap-profile
    set handoff-rssi <rssi_int>
    set handoff-sta-thresh <clients_int>
    config radio-1
      set frequency-handoff {disable | enable}
      set ap-handoff {disable | enable}
    end
    config radio-2
      set frequency-handoff {disable | enable}
      set ap-handoff {disable | enable}
    end
  end
```

Where:

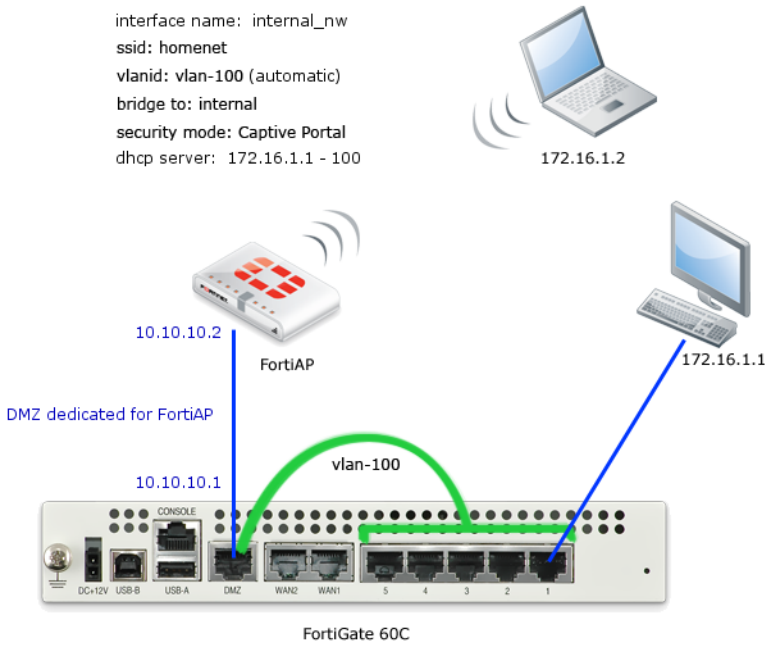
- `handoff-rssi` is the RSSI threshold. Clients with a 5 Ghz RSSI threshold over this value are load balanced to the 5GHz frequency band. Default is 25. Range is 20 to 30.
- `handoff-sta-thresh` is the access point handoff threshold. If the access point has more clients than this threshold it is considered busy and clients are changed to another access point. Default is 30, range is 5 to 25.
- `frequency-handoff` enable or disable frequency handoff load balancing for this radio. Disabled by default.
- `ap-handoff` enable or disable access point handoff load balancing for this radio. Disabled by default.

Frequency handoff must be enabled on the 5GHz radio to learn client capability.

Bridge SSID to FortiGate wired network

A WiFi network can be combined with a wired LAN so that WiFi and wired clients are on the same subnet. This is a convenient configuration for users.

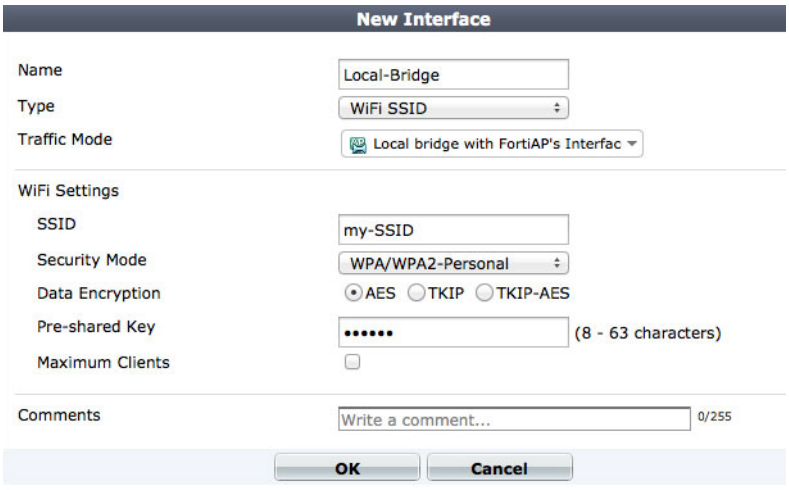
Figure 56:A FortiAP unit bridged with the internal network



This configuration cannot be used in conjunction with Wireless Mesh features because it enables the FortiAP Local Bridge option.

To create the bridged WiFi and wired LAN configuration, you need to configure the SSID with the Local Bridge option so that traffic is sent directly over the FortiAP unit's Ethernet interface to the FortiGate unit, instead of being tunneled to the WiFi controller.

Figure 57:SSID configured with Local Bridge option



Enter the following command from the CLI:

```
config wireless-controller vap
  edit "homenet_if"
    set vdom "root"
    set ssid "homenet"
    set local-bridging enable
    set security wpa-personal
    set passphrase "Fortinet1"
  end
config wireless-controller wtp
  edit FAP22B3U11005354
    set admin enable
    set vaps "homenet_if"
  end
```

IPv6

In order to configure IPv6 features using the web-based manager, IPv6 must be enabled using Feature Select. For more information, see “Feature Select” on page 168.

The following new IPv6 features are available from the FortiOS 5.0 web-based manager:

- IPv6 Policy routing
- IPv6 security policies
- IPv6 Explicit web proxy
- IPv6 NAT – NAT64, DNS64, NAT66
- IPv6 Forwarding Policies - IPS, Application Control, and flow-based antivirus, web filtering and DLP
- New Fortinet FortiGate IPv6 MIB fields
- IPv6 Per-IP traffic shaper
- DHCPv6 relay
- FortiGate interfaces can get IPv6 addresses from an IPv6 DHCP server

IPv6 Policy routing

IPv6 policy routing functions in the same was as IPv4 policy routing. To add an IPv6 policy route, go to *Router* > *Static* > *Policy Routes* and select *Create New* > *IPv6 Policy Route*.

Figure 58:IPv6 policy route

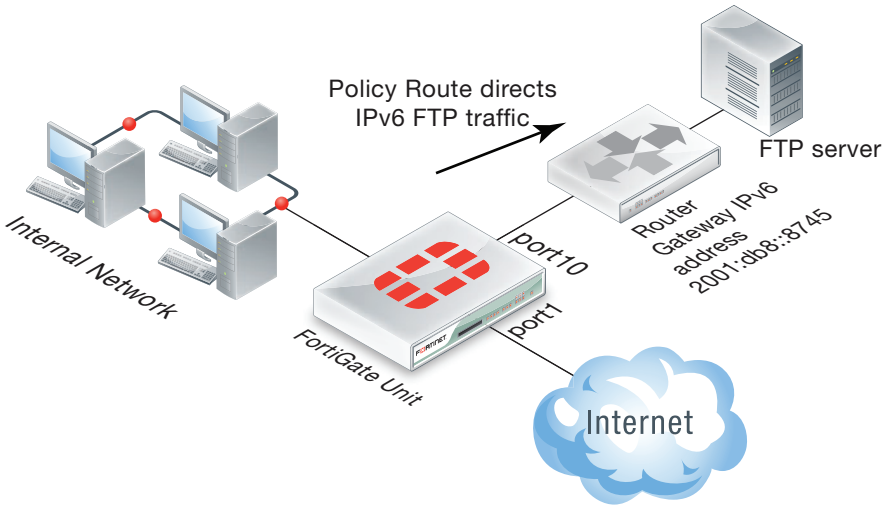
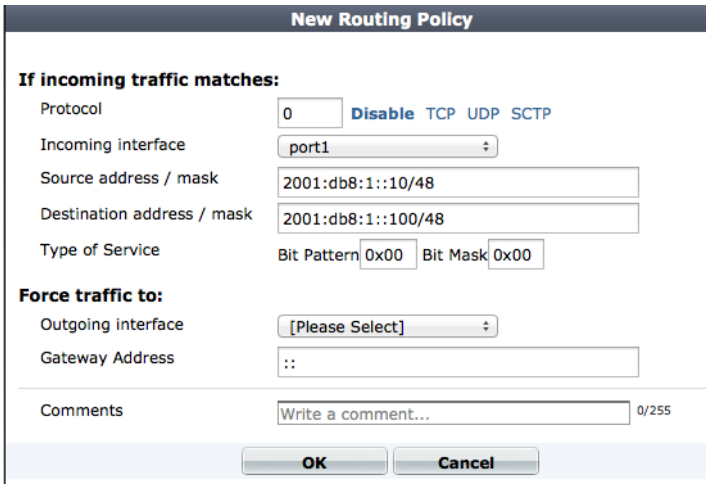


Figure 59: Adding an IPv6 Policy route



You can also use the following command to add IPv6 policy routes:

```
config router policy6
  edit 0
    set input-device <interface>
    set src <ipv6_ip>
    set dst <ipv6_ip>
    set protocol <0-255>
    set gateway <ipv6_ip>
    set output-device <interface>
    set tos <bit_pattern>
    set tos-mask <bit_mask>
  end
```

IPv6 security policies

IPv6 security policies now support all the features supported by IPv4 security policies. The following new features were added in FortiOS 5.0:

- Policy types and subtypes.
- NAT support including using the destination interface IP address, fixed port, and dynamic IP pools.
- All security features (antivirus, web filtering, application control, IPS, email filtering, DLP, VoIP and ICAP).
- All traffic shaping options, including shared traffic shaping, reverse shared traffic shaping and per-IP traffic shaping.
- All user and device authentication options.

IPv6 Explicit web proxy

With FortiOS 5.0, you can use the explicit web proxy for IPv6 traffic. To do this you need to:

- Enable the Explicit Proxy from the System Information dashboard widget.
- Enable the IPv6 explicit web proxy from the CLI.
- Enable the explicit web proxy for one or more FortiGate interfaces. These interfaces also need IPv6 addresses.
- Add IPv6 web proxy security policies to allow the explicit web proxy to accept IPv6 traffic.

Use the following steps to set up a FortiGate unit to accept IPv6 traffic for the explicit web proxy at the Internal interface and forward IPv6 explicit proxy traffic out the wan1 interface to the Internet.

1. Enter the following CLI command to enable the IPv6 explicit web proxy:

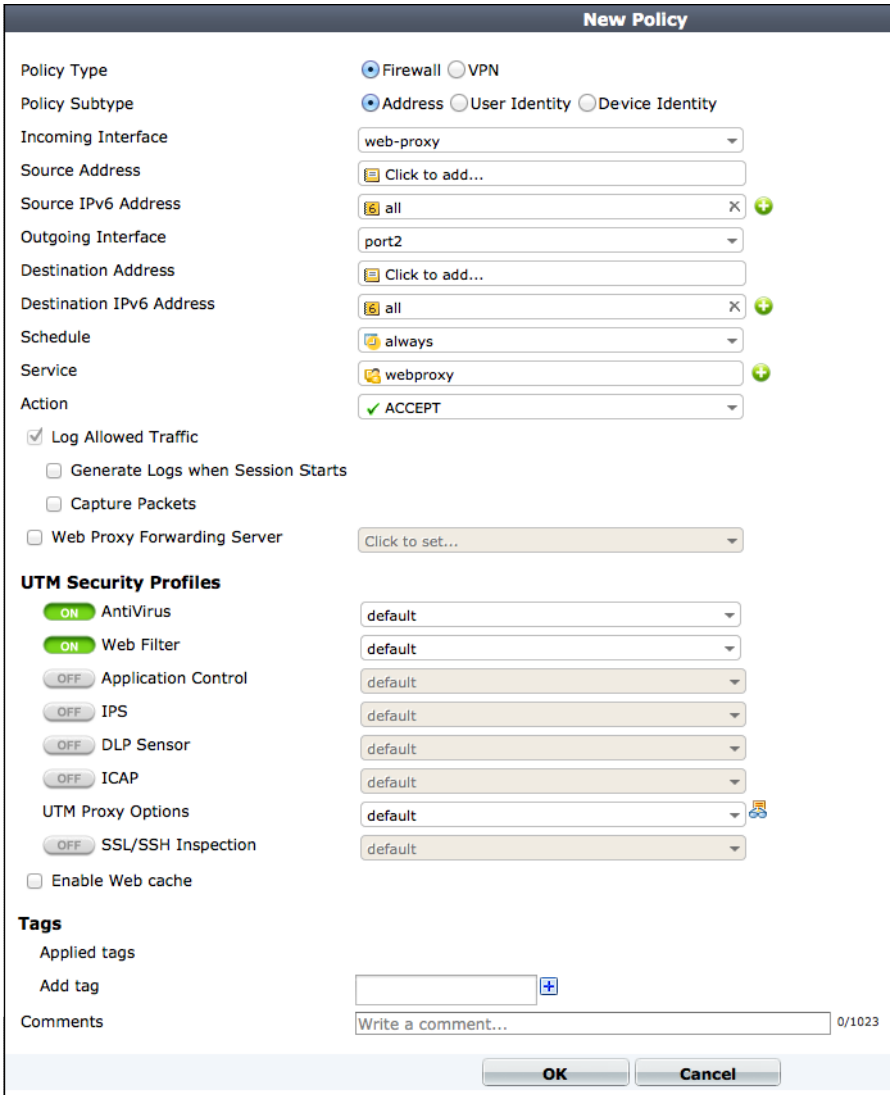
```
config web-proxy explicit
  set status enable
  set ipv6-status enable
end
```

2. Go to *System* > *Network* > *Interfaces* and edit the *internal* interface, select *Enable Explicit Web Proxy* and select *OK*.
3. Go to *Policy* > *Policy* > *IPv6 Policy* and select *Create New* to add an IPv6 explicit web proxy security policy with the following settings shown in Figure 60.

   This IPv6 explicit web proxy policy allows traffic from all IPv6 IP addresses to connect through the explicit web proxy and through the wan1 interface to any IPv6 addresses that are accessible from the wan1 interface.

If you have enabled both the IPv4 and the IPv6 explicit web proxy you can combine IPv4 and IPv6 addresses in a single explicit web proxy policy to allow both IPv4 and IPv6 traffic through the proxy.

Figure 60: Example IPv6 Explicit Web Proxy security policy



Restricting the IP address of the explicit IPv6 web proxy

You can use the following command to restrict access to the IPv6 explicit web proxy using only one IPv6 IP address. The IPv6 address that you specify must be the IPv6 address of an interface that the explicit HTTP proxy is enabled on. You might want to use this option if the explicit web proxy is enabled on an interface with multiple IPv6 addresses.

For example, to require uses to connect to the IPv6 address 2001:db8:0:2::30 to connect to the explicit IPv6 HTTP proxy:

```
config web-proxy explicit
  set incoming-ipv6 2001:db8:0:2::30
end
```

Restricting the outgoing source IP address of the IPv6 explicit web proxy

You can use the following command to restrict the source address of outgoing web proxy packets to a single IPv6 address. The IP address that you specify must be the IPv6 address of an interface that the explicit HTTP proxy is enabled on. You might want to use this option if the explicit HTTP proxy is enabled on an interface with multiple IPv6 addresses.

For example, to restrict the outgoing packet source address to 2001:db8:0:2::50:

```
config http-proxy explicit
  set outgoing-ip6 2001:db8:0:2::50
end
```

IPv6 NAT – NAT64, DNS64, NAT66

NAT66, NAT64 and DNS64 are now supported for IPv6. These options provide IPv6 NAT and DNS capabilities IPv6-IPv4 tunnelling or dual stack configurations. These are available only in the CLI.

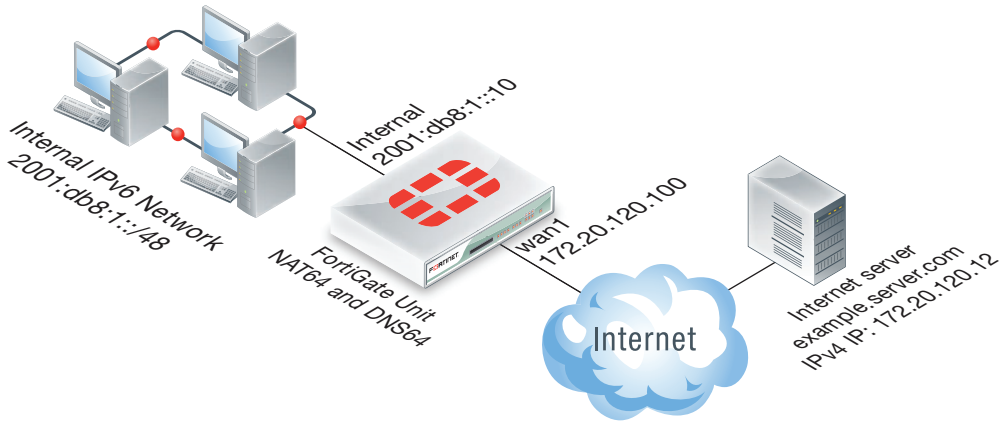
Fortinet supports all features described in RFC 6146. However, for DNS64 there is no support for handling Domain Name System Security Extensions (DNSSEC). DNSSEC is for securing types of information that are provided by the DNS as used on an IP network or networks. You can find more information about DNS64 in RFC 6147.

NAT64 and DNS64

NAT64 is used to translate IPv6 addresses to IPv4 addresses so that a client on an IPv6 network can communicate transparently with a server on an IPv4 network. NAT64 is usually implemented in combination with DNS64. DNS64 synthesizes AAAA records from A records and is used to synthesize IPv6 addresses for hosts that only have IPv4 addresses.

With a NAT64 and DNS64 configuration in place on a FortiGate unit, clients on an IPv6 network can transparently connect to addresses on an IPv4 network. NAT64 and DNS64 perform IPv4 to IPv6 transition, allowing clients that have already switched to IPv6 addresses to continue communicating with servers that still use IPv4 addresses.

Figure 61: Example NAT64 configuration



To configure NAT64 to allow a host on the IPv6 network to connect to the Internet server

In this example the Internal IPv6 network address is 2001:db8:1::/48 and the external IPv4 network address is 172.20.120.0/24. NAT64 is configured to allow a user on the internal network to connect to the server at IPv4 address 172.20.120.12. In this configuration, sessions exiting the wan1 interface must have their source address changed to and IPv4 address in the range 172.20.120.200 to 172.20.120.210.

1. Enter the following command to enable NAT64.

```
config system nat64
  set status enable
end
```

Enabling NAT64 with the `config system nat64` command means that all IPv6 traffic received by the current VDOM can be subject to NAT64 if the source and destination address matches an NAT64 security policy.

By default, the setting `always-senthetize-aaaa-record` is not enabled. With this setting disabled, the DNS proxy will attempt to find an AAAA records for queries to domain names and therefore resolve the host names to IPv6 addresses. If the DNS proxy cannot find an AAAA record, it synthesizes one by adding the NAT64 prefix to the A record.

By using the `nat64-prefix` option of the `config system nat64` command to change the default nat64 prefix (the default is the well known prefix 64:ff9b::/96) and setting `always-senthetize-aaaa-record` to enable, the DNS proxy does not check for AAAA records and always synthesizes AAAA records.

As an alternative to the above entry, there is the optional configuration that would allow the resolution of CNAME queries.

```
config system nat64
  set status enable
  set nat64-prefix 64:ff9b::/96
  set always-synthesize-aaaa-record enable
end
```

2. Enter the following command to add an IPv6 firewall address for the internal network:

```
config firewall address6
  edit internal-net6
    set ip6 2001:db8::/48
  end
```

3. Enter the following command to add an IPv4 firewall address for the external network:

```
config firewall address
  edit external-net4
    set subnet 172.20.120.0/24
    set associated-interface wan1
  end
```

4. Enter the following command to add an IP pool containing the IPv4 address that the should become the source address of the packets exiting the wan1 interface:

```
config firewall ippool
  edit exit-pool4
    set startip 172.20.120.200
    set endip 172.20.120.210
  end
```

5. Enter the following command to add a NAT64 policy that allows connections from the internal IPv6 network to the external IPv4 network:

```
config firewall policy64
  edit 0
    set srcintf internal
    set srcaddr internal-net6
    set dstintf wan1
    set dstaddr external-net4
    set action accept
    set schedule always
    set service ANY
    set logtraffic enable
    set ippool enable
    set poolname exit-pool4
  end
```

The `srcaddr` can be any IPv6 firewall address and the `dstaddr` can be any IPv4 firewall address.

Other NAT64 policy options include `fixedport`, that can be used to prevent NAT64 from changing the destination port. You can also configure traffic shaping for NAT64 policies.

How a host on the internal IPv6 network communicates with example.server.com that only has IPv4 address on the Internet

1. The host on the internal network does a DNS lookup for example.server.com by sending a DNS query for an AAAA record for example.server.com.
2. The DNS query is intercepted by the FortiGate DNS proxy.
3. The DNS proxy attempts to resolve the query with a DNS server on the Internet and discovers that there are no AAAA records for example.server.com.

The previous step is skipped if `always-senthetize-aaaa-record` is enabled.

4. The DNS proxy performs an A-record query for example.server.com and gets back an RRSet containing a single A record with the IPv4 address 172.20.120.12.
5. The DNS proxy then synthesizes an AAAA record. The IPv6 address in the AAAA record begins with the configured NAT64 prefix in the upper 96 bits and the received IPv4 address in the lower 32 bits. By default, the resulting IPv6 address is 64:ff9b::172.20.120.12.
6. The host on the internal network receives the synthetic AAAA record and sends a packet to the destination address 64:ff9b::172.20.120.12.
7. The packet is routed to the FortiGate internal interface where it is accepted by the NAT64 security policy.
8. The FortiGate unit translates the destination address of the packets from IPv6 address 64:ff9b::172.20.120.12 to IPv4 address 172.20.120.12 and translates the source address of the packets to 172.20.120.200 (or another address in the IP pool range) and forwards the packets out the wan1 interface to the Internet.

NAT66

NAT66 is used for translating an IPv6 source or destination address to a different IPv6 source or destination address. NAT66 is not as common or as important as IPv4 NAT, as many IPv6 IP addresses do not need NAT66 as much as IPv4 NAT. However, NAT66 can be useful for a number of reasons. For example, you may have changed the IP addresses of some devices on your network but want traffic to still appear to be coming from their old addresses. You can use NAT66 to translate the source addresses of packets from the devices to their old source addresses.

In FortiOS 5.0, NAT66 options can be added to an IPv6 security policy from the CLI.

Configuring NAT66 is very similar to configuring NAT in an IPv4 security policy. For example, use the following command to add an IPv6 security policy that translates the source address of IPv6 packets to the address of the destination interface (similar to IPv4 source NAT:

```
config firewall policy6
  edit 0
    set srcintf internal
    set dstintf wan1
    set srcaddr internal_net
    set dstaddr all
    set action accept
    set schedule always
    set service ANY
    set nat enable
  end
```

Its also can be useful to translate one IPv6 source address to another address that is not the same as the address of the exiting interface. You can do this using IP pools. For example, enter the following command to add an IPv6 IP pool containing one IPv6 IP address:

```
configure firewall ippool6
  edit example_6_pool
    set startip 2001:db8::
    set endip 2001:db8::
  end
```

Enter the following command to add an IPv6 firewall address that contains a single IPv6 IP address.

```
configure firewall address6
  edit device_address
    set ip6 2001:db8::132/128
  end
```

Enter the following command to add an IPv6 security policy that accepts packets from a device with IP address 2001:db8::132 and translates the source address to 2001:db8::.

```
config firewall policy6
  edit 0
    set srcintf internal
    set dstintf wan1
    set srcaddr device_address
    set dstaddr all
    set action accept
    set schedule always
    set service ANY
    set nat enable
    set ippool enable
    set poolname example_6_pool
  end
```

NAT66 destination address translation

NAT66 can also be used to translate destination addresses. This is done in an IPv6 policy by using IPv6 virtual IPs. For example, enter the following command to add an IPv6 virtual IP that maps destination address 2001:db8::dd to 2001:db8::ee

```
configure firewall vip6
  edit example-vip6
    set extip 2001:db8::dd
    set mappedip 2001:db8::ee
  end
```

Enter the following command to add an IPv6 security policy that accepts packets with a destination address 2001:db8::dd and translates that destination address to 2001:db8::ee

```
config firewall policy6
  edit 0
    set srcintf internal
    set dstintf wan1
    set srcaddr all
    set dstaddr example-vip6
    set action accept
    set schedule always
    set service ANY
  end
```

IPv6 Forwarding Policies - IPS, Application Control, and flow-based antivirus, web filtering and DLP

FortiOS 5.0 fully supports flow-based inspection of IPv6 traffic. This includes full support for IPS, application control, as well as flow-based virus scanning, and web filtering.

To add flow-based inspection to IPv6 traffic go to *Policy* > *Policy* > *IPv6 Policy* and select *Create New* to add an IPv6 Security Policy. Configure the policy to accept the traffic to be scanned. Select UTM and select the UTM profiles to apply to the traffic. To apply flow-based

inspection you can select an IPS and an application control profile. You can also select antivirus or web filtering profiles in which flow-based inspection has been selected.

New Fortinet FortiGate IPv6 MIB fields

The following IPv6 MIB fields have been added to the Fortinet FortiGate MIB. These MIS entries can be used to display IPv6 session and policy statistics.

- IPv6 Session Counters:
  `fgSysSes6Count`
  `fgSysSes6Rate1`
  `fgSysSes6Rate10`
  `fgSysSes6Rate30`
  `fgSysSes6Rate60`
- IPv6 Policy Statistics:
  `fgFwPol6StatsTable`
  `fgFwPol6StatsEntry`
  `FgFwPol6StatsEntry`
  `fgFwPol6ID`
  `fgFwPol6PktCount`
  `fgFwPol6ByteCount`
- IPv6 Session Statistics:
  `fgIp6SessStatsTable`
  `fgIp6SessStatsEntry`
  `FgIp6SessStatsEntry`
  `fgIp6SessNumber`

The fgSysSesCount and fgSysSesRateX MIBs report statistics for IPv4 plus IPv6 sessions combined. This behavior was not changed.

New OIDs

The following OIDs have been added:

```
FORTINET-FORTIGATE-MIB:fortinet.fnFortiGateMib.fgSystem.fgSystemInfo
.fgSysSes6Count   1.3.6.1.4.1.12356.101.4.1.15
.fgSysSesRate1    1.3.6.1.4.1.12356.101.4.1.16
.fgSysSesRate10   1.3.6.1.4.1.12356.101.4.1.17
.fgSysSesRate30   1.3.6.1.4.1.12356.101.4.1.18
.fgSysSesRate60   1.3.6.1.4.1.12356.101.4.1.19

FORTINET-FORTIGATE-MIB:fortinet.fnFortiGateMib.fgFirewall.fgFwPolicies
     .fgFwPolTables
.fgFwPol6StatsTable.fgFwPol6StatsEntry.fgFwPol6ID   1.3.6.1.4.1.12356.
     101.5.1.2.2.1.1
.fgFwPol6StatsTable.fgFwPol6StatsEntry.fgFwPol6PktCount   1.3.6.1.4.1.
     12356.101.5.1.2.2.1.2
.fgFwPol6StatsTable.fgFwPol6StatsEntry.fgFwPol6ByteCount   1.3.6.1.4.1
     .12356.101.5.1.2.2.1.3

FORTINET-FORTIGATE-MIB:fortinet.fnFortiGateMib.fgInetProto.fgInetProto
     Tables
.fgIp6SessStatsTable.fgIp6SessStatsEntry.fgIp6SessNumber
     1.3.6.1.4.1.12356.101.11.2.3.1.1
```

EXAMPLE SNMP get/walk output

```
// Session6 stats excerpt from sysinfo:
snmpwalk -v2c -cpublic 192.168.1.111 1.3.6.1.4.1.12356.101.4
FORTINET-FORTIGATE-MIB::fgSysSes6Count.0 = Gauge32: 203
FORTINET-FORTIGATE-MIB::fgSysSes6Rate1.0 = Gauge32: 10 Sessions Per
     Second
FORTINET-FORTIGATE-MIB::fgSysSes6Rate10.0 = Gauge32: 2 Sessions Per
     Second
FORTINET-FORTIGATE-MIB::fgSysSes6Rate30.0 = Gauge32: 1 Sessions Per
     Second
FORTINET-FORTIGATE-MIB::fgSysSes6Rate60.0 = Gauge32: 0 Sessions Per
     Second

// FwPolicy6 table:
snmpwalk -v2c -cpublic 192.168.1.111 1.3.6.1.4.1.12356.101.5.1.2.2
FORTINET-FORTIGATE-MIB::fgFwPol6ID.1.3 = INTEGER: 3
FORTINET-FORTIGATE-MIB::fgFwPol6ID.1.4 = INTEGER: 4
FORTINET-FORTIGATE-MIB::fgFwPol6PktCount.1.3 = Counter64: 4329
FORTINET-FORTIGATE-MIB::fgFwPol6PktCount.1.4 = Counter64: 0
FORTINET-FORTIGATE-MIB::fgFwPol6ByteCount.1.3 = Counter64: 317776
FORTINET-FORTIGATE-MIB::fgFwPol6ByteCount.1.4 = Counter64: 0

// IP6SessNumber:
snmpwalk -v2c -cpublic 192.168.1.111 1.3.6.1.4.1.12356.101.11.2.3.1
FORTINET-FORTIGATE-MIB::fgIp6SessNumber.1 = Counter32: 89
```

IPv6 Per-IP traffic shaper

You can add any Per-IP traffic shaper to an IPv6 security policy using the following command:

```
config firewall policy6
  edit 0
    set per-ip-shaper 'new-perip-shaper'
  end
```

DHCPv6 relay

You can use the following command to configure a FortiGate interface to relay DHCPv6 queries and responses from one network to a network with a DHCPv6 server and back. The command enables DHCPv6 relay and includes adding the IPv6 address of the DHCP server that the FortiGate unit relays DHCPv6 requests to:

```
config system interface
  edit internal
    config ipv6
      set dhcp6-relay-service enable
      set dhcp6-relay-type regular
      set dhcp6-relay-ip 2001:db8:0:2::30
  end
```

FortiGate interfaces can get IPv6 addresses from an IPv6 DHCP server

From the CLI you can configure any FortiGate interface to get an IPv6 address from an IPv6 DHCP server. For example, to configure the wan2 interface to get an IPv6 address from an IPv6 DHCP server enter the following command:

```
config system interface
  edit wan2
    config ipv6
      set ip6-mode dhcp
    end
end
```

Logging and reporting

New logging and reporting features include:

- Log message reorganization
- Log Viewer Improvements
- The FortiGate Security Analysis Report
- Converting compact log format

FortiCloud, the new logging and reporting feature that replaces FAMS, is described in FortiOS 5.0 *Installation and System Administration*.

Log message reorganization

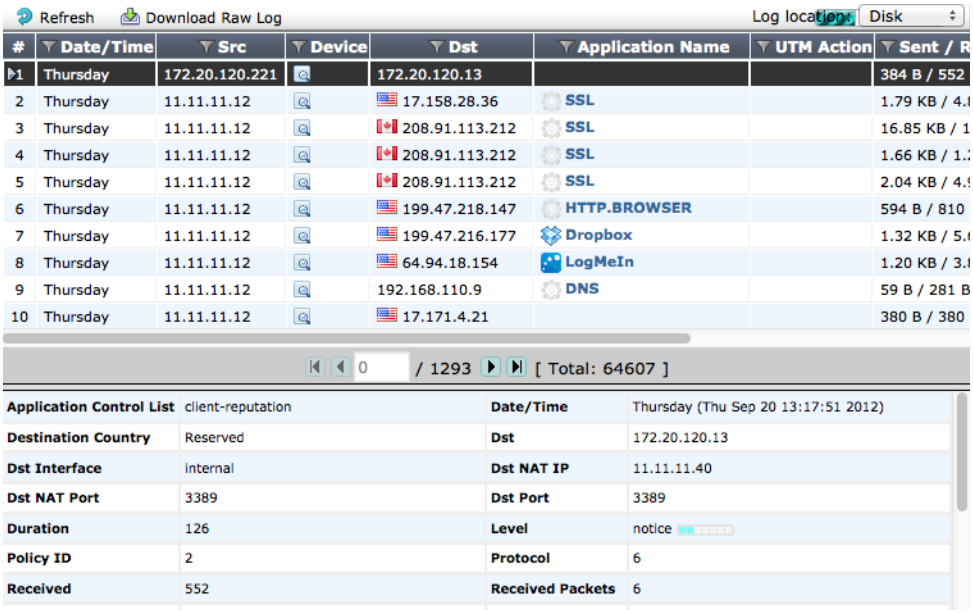
FortiOS 5.0 log messages have been re-organized. The new log message format will be described in the FortiOS 5.0 *Logging and Reporting Guide* and *Log Message Reference*.

Log Viewer Improvements

In FortiOS 5.0, the Log & Report menu provides access to the following types of log messages:

- Traffic log
  - Forward Traffic - log messages for traffic passing through the FortiGate unit. Includes traffic log messages as well as Security log messages so that you can view messages about Security events (such as a message indicating that a virus was found) in the same location as the traffic log messages that recorded the current traffic at the time. From the forward traffic log viewer, you can also view content logs and quarantined files. Forward traffic log messages also include log messages created when you enable logging for the IPv4 and IPv6 security policy implicit security policies.
  - Local Traffic - Log messages for traffic terminating at the FortiGate unit. All traffic terminating at the FortiGate unit is allowed or denied by a local in policy. To view local in policies go to *Policy* > *Policy* > *Local In Policy*. You can enable and disable logging for local in traffic from here as well.
  - Multicast Traffic - Log messages for multicast traffic passing through the FortiGate unit and allowed by multicast traffic policies
  - Invalid Packets - Log messages recorded when the FortiGate unit receives invalid packets.
- Event log - Event log messages organized into the following categories:
  - System
  - Router
  - VPN
  - User
  - WAN Opt. & Cache
  - WiFi

Figure 62: Example Forward Traffic log display showing some Security log messages



From each of these log message viewers, you can download raw log messages, adjust the column settings to display the ones you are most interested in, filter the messages according to a wide range of criteria and display detailed information for a selected log message. In addition, you can control the source of the log messages that are displayed. For example, setting the log location source can be the disk, if your FortiGate unit has available internal storage.

Other logging improvements include:

- New event log types including event logs for FortiClient usage.
- Traffic log messages for packets blocked by the implicit policies that appear at the bottom of IPv4 and IPv6 policy lists. You can enable logging for these policies by editing them and selecting *Log Violation Traffic*.
- When you enable logging on a security policy and a session begins, the FortiGate unit logs that session as well as logging when that session closes. These traffic logs contain the log fields status=start, when a session has started, and status=close, when the session ends.
- Email filter log messages now contain a new field, the cc field, which provides all the email addresses that were copied (or cc'd) to the original email message.
- There are two new event logs that contain information about the FSSO polling daemon: one event log is recorded when a logged on user adds or replaces an old user; the second event log is recorded when an old user is logged off because of inactivity or when replaced.

From the CLI, all of these and some other options are available from the new `config log setting` command. This command configures traffic logging settings per VDOM.

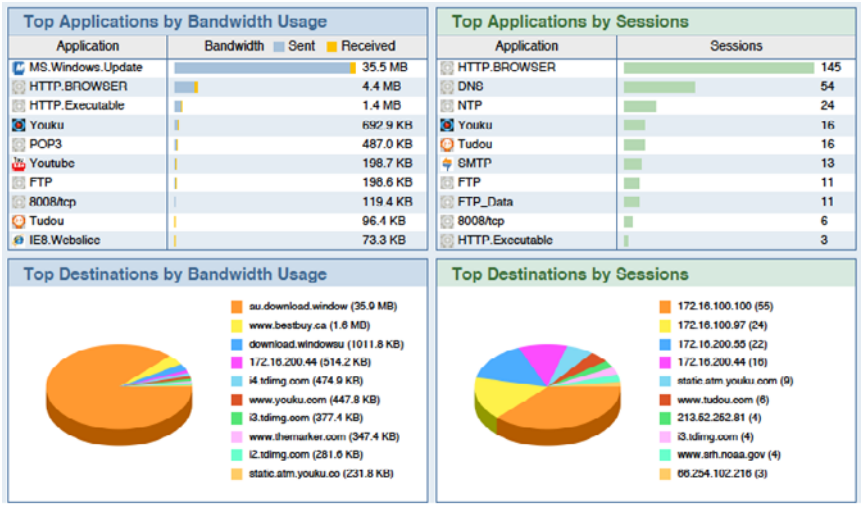
The FortiGate Security Analysis Report

In order for your FortiGate unit to create a Security Analysis Report, disk logging must be enabled. To enable disk logging, go to *Log & Report* > *Log Config* > *Log Settings* and under *Logging and Archiving* select *Disk* and *Enable Local Reports*.

Viewing the current report

You can go to *Log & Report* > *Report* > *Local* and select *Run Now* to view the latest FortiGate Security Analysis Report. This report is constantly updated so you can go here any time to get the current report. The Multi-page report provides wide range of data including bandwidth and application use, users, destinations, streaming usage, email traffic, and so on.

Figure 63: Extract from a sample report



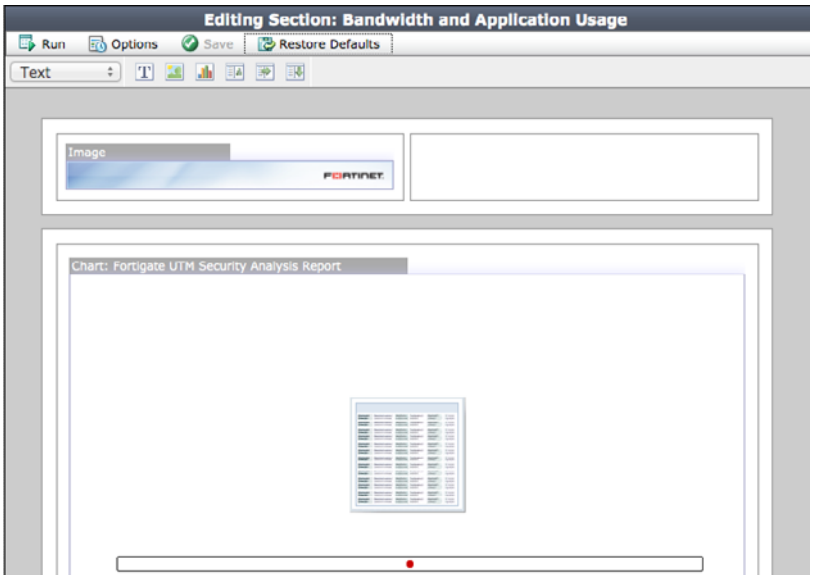
Viewing the saved (historical) security analysis reports

You can go to *Log & Report* > *Report* > *Local* to select saved reports to view.

Customizing the security analysis report

You can go to *Log & Report* > *Report* > *Local* and select *Customize* to customize the look and content of the report. You can also change the report schedule and other options.

Figure 64: Customizing report look and content



Select *Options* to change the report schedule to Daily, Weekly or On Demand. You can also change the time of day at which an old report is saved and a new one started.

Converting compact log format

To convert your compact logs to the new FortiOS 5 format, use the following CLI command:

```
execute log convert-oldlogs
```

This command is available only if you have upgraded from an earlier version of FortiOS and have old compact logs on your system.

Firewall

New firewall features include:

- Choosing the policy type
- Reorganized Firewall Services
- Local in policies
- Multicast Policies
- Adding DoS Anomaly protection to a FortiGate interface
- Changes to security proxy options
- SSL and SSH inspection

Choosing the policy type

Creating and editing security policies has been enhanced make creating different types of security policies easier to understand. Now the first step in creating a security policy, after going to *Policy* > *Policy* > *Policy* and selecting *Create New* is to select the *Policy Type* (Firewall or VPN) and *Policy Subtype*. The policy subtype selections depend on the policy type:

- If you select *Firewall* you can also select
  - *Address* to create a basic security policy
  - *User Identity* to create a policy that identifies users (user authentication)
  - *Device Identity* to create a policy that identifies devices (device authentication or BYOD)
- If you select *VPN* you can also select
  - *IPsec* to create IPsec VPN policies
  - *SSL-VPN* to create SSL VPN policies

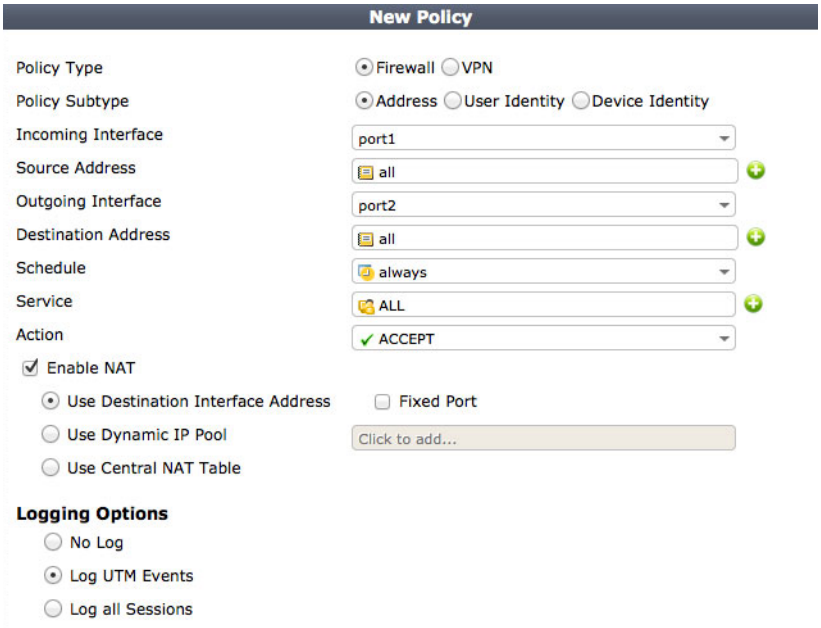
This section describes:

- Creating a basic security policy
- Creating a security policy to authenticate users
- Creating a security policy to authenticate devices for BYOD
- Creating a policy-based IPsec VPN security policy
- Creating a route-based IPsec VPN security policy
- Creating an SSL VPN security policy

Creating a basic security policy

Use the default policy type settings to create a basic security policy. Select incoming and outgoing interfaces, source and destination addresses, the schedule, services and the action. Select other features such as NAT, logging, Security Features and so on.

Figure 65: Creating a basic security policy



Creating a security policy to authenticate users

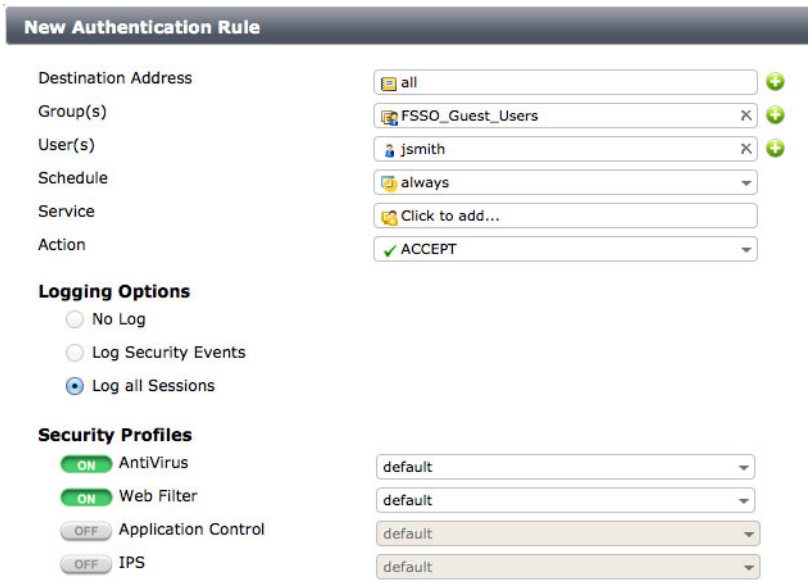
Select the *Firewall* policy type and the *User Identity* subtype. Select incoming and outgoing interfaces, source addresses, and other features. Then select *Create New* to add a user authentication rule to the policy.

User authentication rules include destination addresses, user groups and or individual users, a schedule, services, the action, logging settings, and UTM security profiles.

You select the destination address separately for each authentication rule. This means that you can apply different features to different user groups depending on their destination addresses.

You can also now add individual users to authentication rules instead of just user groups.

Figure 66: Adding a user authentication rule

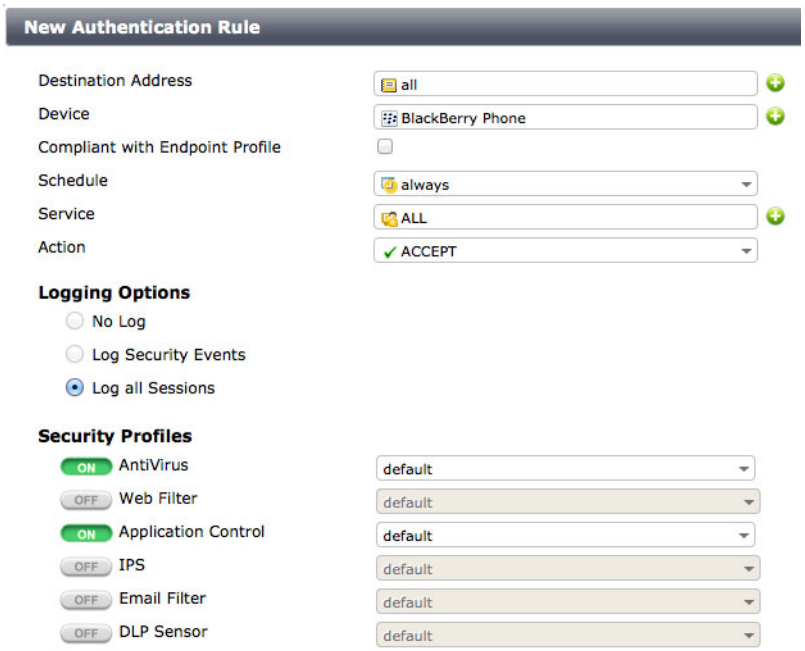


Creating a security policy to authenticate devices for BYOD

Select the *Firewall* policy type and the *Device Identity* subtype. Select incoming and outgoing interfaces, source addresses, and other features. Then select *Create New* to add device authentication rules to the policy.

Device authentication rules include the destination address, user groups and or individual users, schedule, service, action, logging, and UTM security profiles.

Figure 67: Adding a device authentication rule



Creating a policy-based IPsec VPN security policy

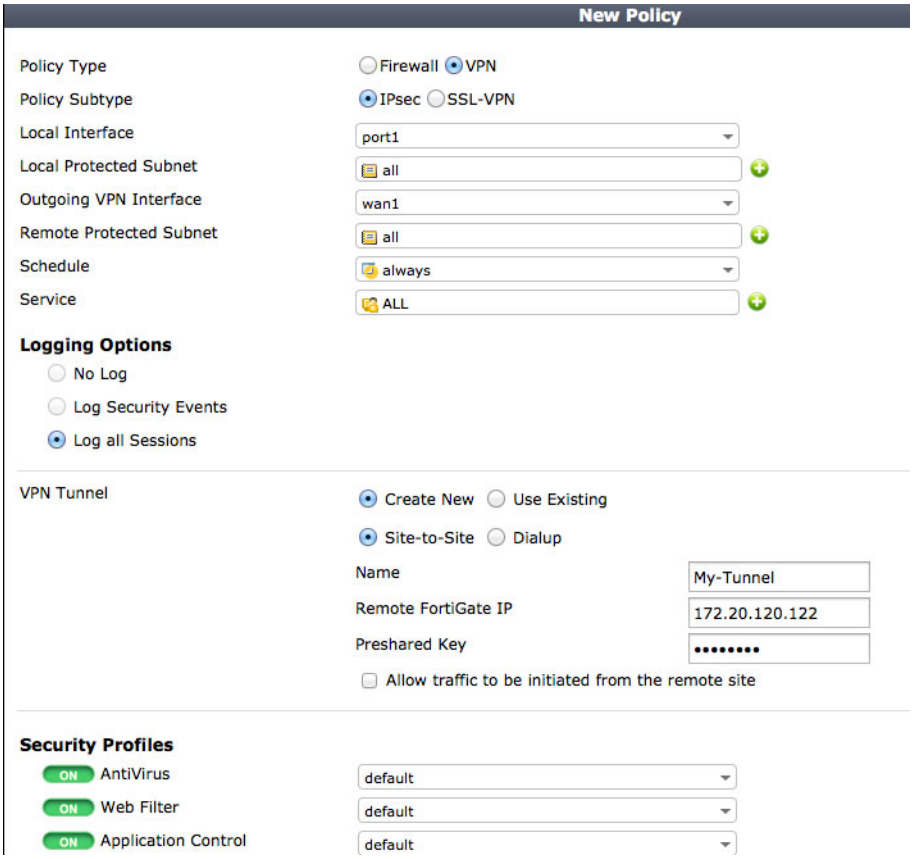
Select the *VPN* policy type and the *IPsec* subtype. Select the local and outgoing VPN interfaces, local protected subnet and remote protected subnet addresses, the schedule, services, and the action.

You have two options to configure the *VPN Tunnel* used by the policy.

- You can use a tunnel that has already been added. Select *Use Existing* and select the tunnel to use.
- You can add a new tunnel. Select *Create New* and select either *Site to Site* or *Dialup*. Add a *Name* for the tunnel, the IP address of the remote FortiGate unit (not required for Dialup) and the Preshared Key to be used by the tunnel.

You can also apply Security Profiles and Client Reputation to IPsec VPN traffic.

Figure 68: Creating a policy-based IPsec VPN policy

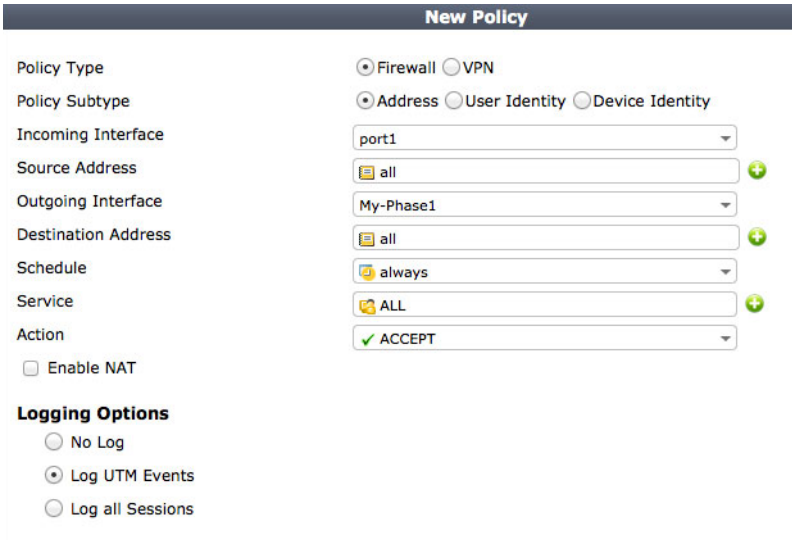


Creating a route-based IPsec VPN security policy

You configure route-based IPsec VPN by first adding a Phase 1 and selecting *Enable IPsec Interface Mode*. This adds an IPsec interface with the same name as the Phase 1.

A security policy for this VPN is a standard security policy that allows traffic between the IPsec interface and another FortiGate unit interface. Create a new policy, select the *Firewall* policy type and the *Address* policy subtype. To allow traffic from the internal network to connect to the VPN, set the incoming interface to internal and the outgoing interface to the IPsec interface. Otherwise configure the security policy like any basic security policy.

Figure 69: Creating a route-based IPsec VPN policy



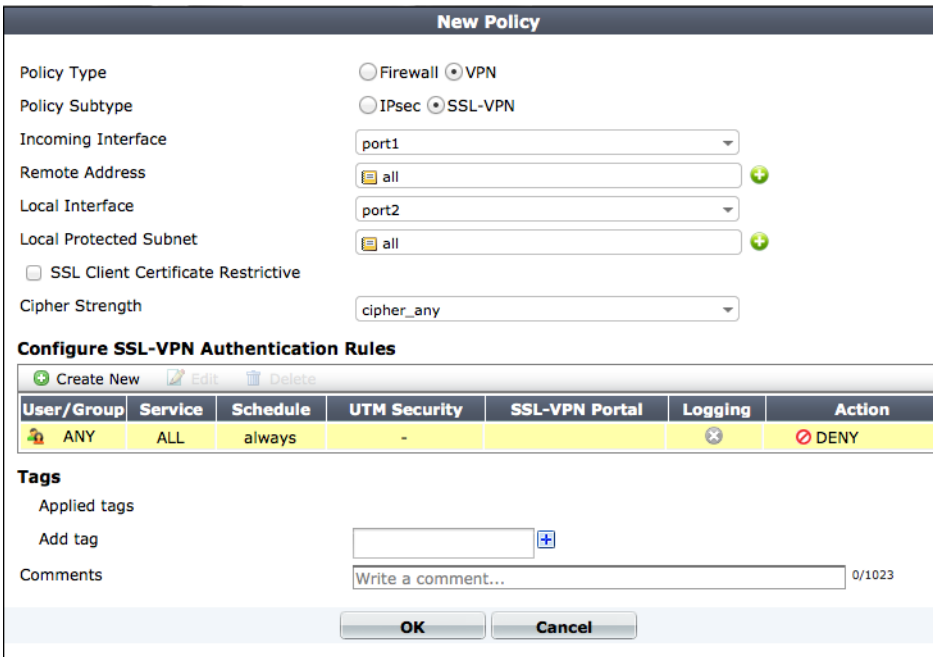
Creating an SSL VPN security policy

Select the *VPN* policy type and the *SSL-VPN* subtype. Select the incoming interface, the remote address, the local interface, and the address for the local protected subnet. Then select *Create New* to add SSL VPN authentication rules to the policy.

SSL authentication rules include user groups, individual users, schedule, service, SSL VPN portal, action, logging, and UTM security profiles.

FortiOS 5.0 no longer includes SSL VPN users or user groups. Any type of user group can be added to an SSL VPN authentication rule.

Figure 70: Creating an SSL VPN policy

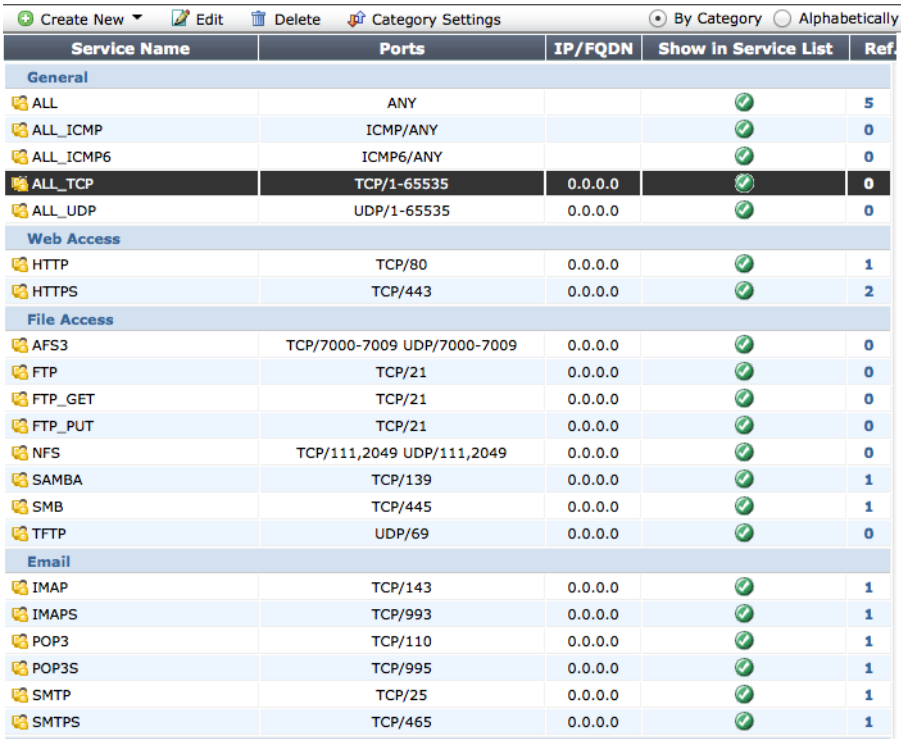


Reorganized Firewall Services

To make Firewall services easier to use and more customizable, the former predefined services list and custom services have been merged into one list and the list has been organized into categories. You can go to *Firewall Objects* > *Service* > *Services* to see the new service list.

The order that the categories and services in the services list is maintained when you add a service to another configuration object, such as a security policy. You can add categories, change the category that a service is in and rearrange the order of categories in the list.

Figure 71: Firewall Services list



The single *ANY* service has been replaced with five *ALL* services that match all services or all services of a specific type (ICMP, ICMP6, TCP and UDP). Otherwise, all of the familiar pre-defined services can be found in the new services list.

By default, the list is organized by categories. You can select *Category Settings* to change the order of the categories in the list. You can also choose to organize the list alphabetically by service name.

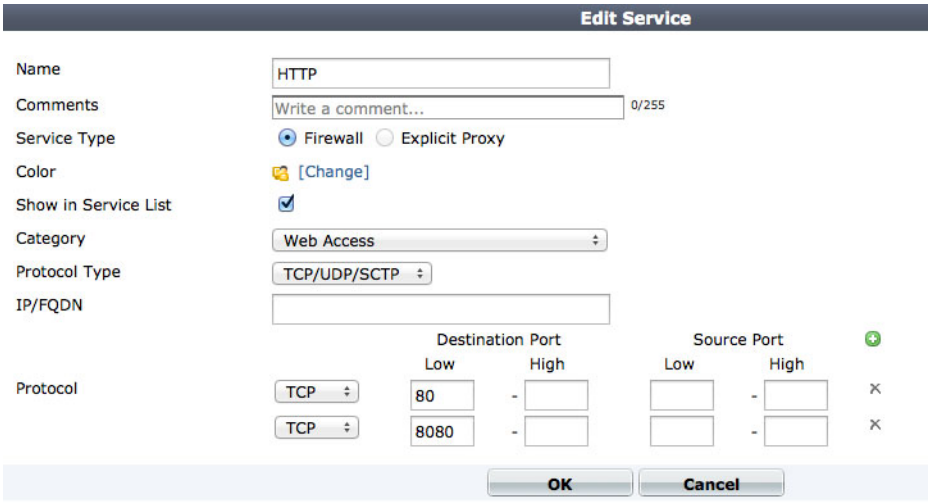
Editing and deleting services

You can edit and delete any of the services in the list; however, use caution when deleting any services. Normally you would only delete a custom service that you have created.

You can edit any service to change its name, add a comment, change its icon color, add or remove it from the list, change its category, change its protocol type, add an IP address or fully qualified domain name (FQDN) and change the source and destination ports for the service.

In most cases, you should not need to edit predefined services. Instead you would add custom services. However, in some cases editing pre-defined services can simplify your configuration. For example, if all of you HTTP traffic uses port 8080, you could edit the HTTP service and change its destination port to 8080. Alternatively, if your network uses port 80 and 8080 for HTTP traffic, you could edit the HTTP service and add port 8080.

Figure 72:HTTP service customized to include port 80 and port 8080



Adding an address to a service

Services now include a IP/FQDN field into which you can add an IP address or a fully qualified domain name. Use this field if you want to restrict the network address that the FortiGate unit will accept connections to this service from.

Adding a new service

To add a new service, go to the service list and select *Create New* > *Service*. Configure the custom service as shown in Figure 72 and select *OK* to save it.

Adding a new service category

If you have a group of services that you use often, you can group them into your own service category to make them easy to find in the list. To add a new service category, go to the service list and select *Create New* > *Category*, add a name for the custom service and select *OK*.

Then select Category Settings and change the order in which the services appear in the list. To make your custom category easy to find, move it to the top of the list.

To add services to your category, edit them and set *Category* to the name of your custom category.

Local in policies

Read-only local in policies show you all the types of traffic that can connect to or terminate at the FortiGate unit. For the FortiGate unit to receive local traffic a policy to receive the traffic must be in the local in policy list. The FortiGate unit needs to be able to receive traffic for a number of reasons. Among them:

- Central management connections from FortiManager
- Networking and routing connections, for example accepting or relaying DHCP requests, accepting routing communication from other routers (for example, OSPF, RIP, VRRP)
- Administrative access to FortiGate interfaces over ICMP, HTTP, HTTPS, and so on.

The local-in policy list includes an action column that shows whether the FortiGate unit accepts or drops sessions identified by the individual local in policies. As you change some

configuration settings those changes are reflected in the local in policies. For example, Administrative Access local in policies change depending on the administrative access settings of your FortiGate interfaces.

From the local in policy page (*Firewall* > *Policy* > *Local In Policy)*, you can enable or disable logging for local in allowed and denied traffic and for local out traffic.

In addition to the pre-defined local in policies, you can add your own using the following command:

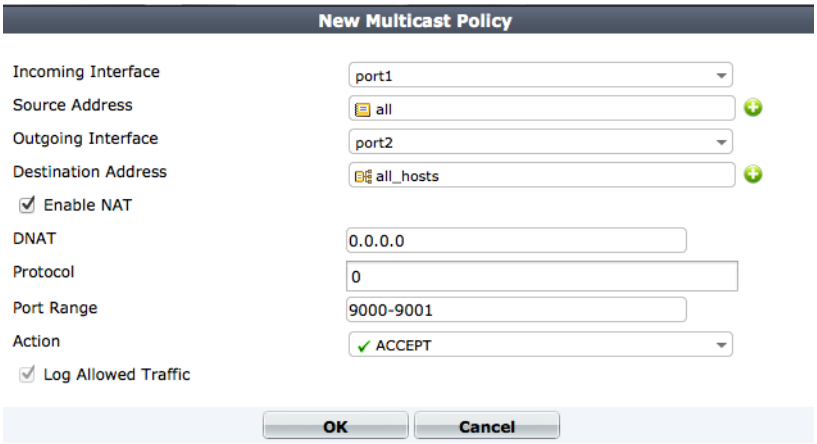
```
config firewall {local-in-policy | local-in-policy6}
  edit 0
    set srcaddr all
    set dstaddr all
    set action {deny | allow}
    set service ALL
    set schedule always
    set auto-asic-offload {disable | enable}
  end
```

Multicast Policies

A number of popular services use multicast protocols. Examples include the Bonjour service used for finding devices on a network, EIGRP and OSPF. To make it easier to allow multicast traffic through the FortiGate unit, you can now add multicast policies from the web-based manager by going to *Policy* > *Policy* > *Multicast Policy* and selecting *Create New*.

Similar to a regular security policy, you configure a multicast policy by selecting incoming and outgoing interfaces, source and destination addresses, enabling NAT, and selecting an action.

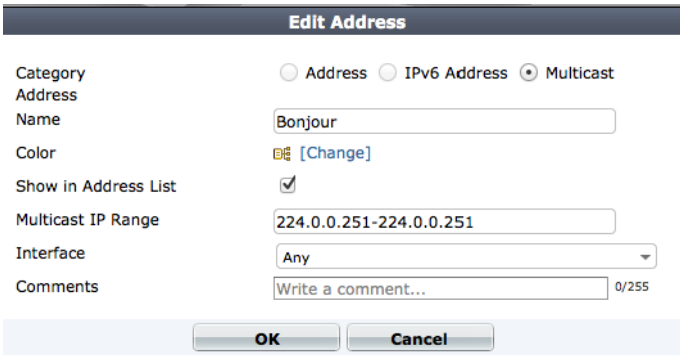
Figure 73: Adding a multicast policy



Specific to multicast policies, you can also specify a destination NAT (DNAT) address and select a multicast protocol (options include ANY, ICMP, IGMP, TCP, UDP, OSPF and other). You cannot add or edit these protocols but, if you select *Other,* you can add a protocol number.

The destination address of a multicast policy must be a multicast address firewall object. Multicast addresses are added by going to *Firewall Objects* > *Address* > *Addresses* and selecting *Create New* > *Multicast Address*. The FortiGate default configuration includes some commonly used multicast addresses. Figure 74 shows the configuration of the default Bonjour multicast address.

Figure 74: Default Bonjour multicast firewall address



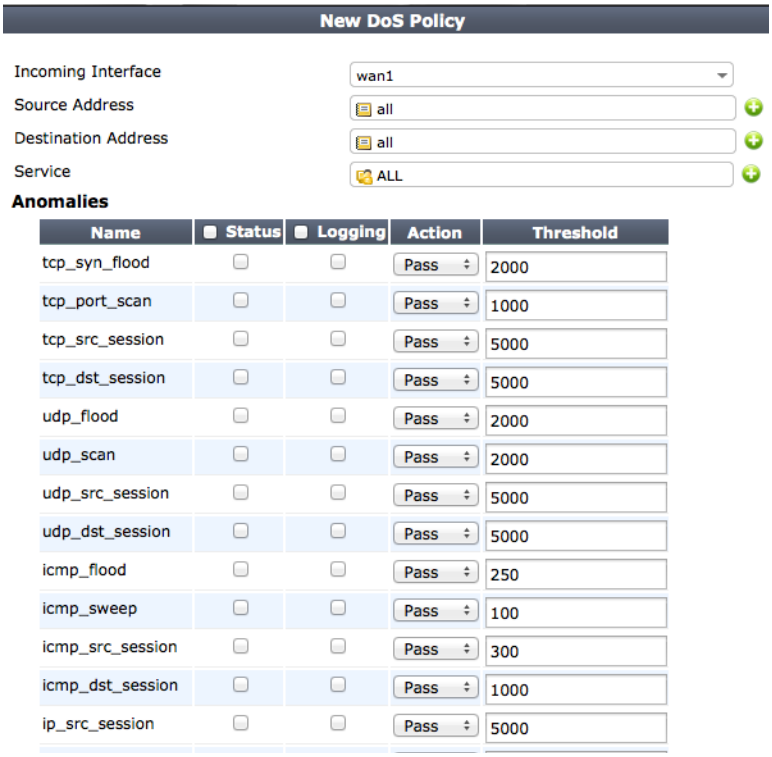
Adding DoS Anomaly protection to a FortiGate interface

New DoS policies allow you to apply DoS anomalies to all traffic that hits a FortiGate interface. This is the only way to apply DoS anomaly protection.

To add a DoS policy go to *Policy* > *Policy* > *DoS Policy* and select Create New to add a new DoS policy. Select the FortiGate interface to add the policy to and select the source and destination addresses and services that will match the packets that you want to apply DoS anomalies to.

Enable one or more DoS anomalies. For each anomaly you can enable logging, set the action to pass or block and change the threshold.

Figure 75: DoS policy



Use the following command to add a DoS policy from the CLI that adds syn flood protection for all traffic hitting the wan2 interface:

```
config firewall DoS-policy
  edit 1
    set interface wan2
    set srcaddr all
    set dstaddr all
    set service ALL
        config anomaly
          edit tcp_syn_flood
            set status enable
            set log enable
            set action block
          end
  end
```

DoS sensors no longer available. DoS policies are the most common method for applying DoS anomalies in FortiOS 5.0.

You can also use the following command to apply DoS anomalies to a one-arm sniffer configuration.

```
config firewall sniffer
```

Interface policies are still available in FortiOS 5.0 from the CLI using the following commands:

```
config firewall interface-policy
config firewall interface-policy6
```

You can use interface policies to apply application control, intrusion protection, virus scanning, web filtering, email filtering and data leak protection to traffic received by an interface.

The following commands are also available for adding sniffer interface policies, which are similar to interface policies:

```
config firewall sniff-interface-policy
config firewall sniff-interface-policy6
```

All of these command have similar syntax for applying Security Features to traffic connecting to or sniffed by a FortiGate interface.

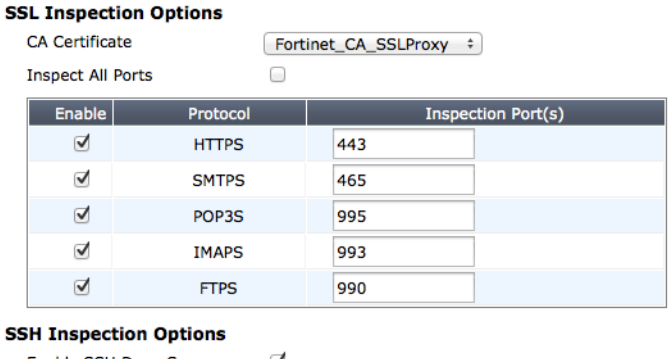
Changes to security proxy options

Security proxy profile options are now configured by feature instead of by protocol. Also, SSL and SSH inspection options have been moved to the new SSL/SSH inspection options profiles.

Protocol port mapping

For all content protocols, you can configure protocol port mapping to set the ports on which the FortiGate unit looks for the protocols. The FortiGate unit can inspect each kind of traffic on any port or you can specify one or more ports.

Figure 76: Configuring Protocol Port Mapping



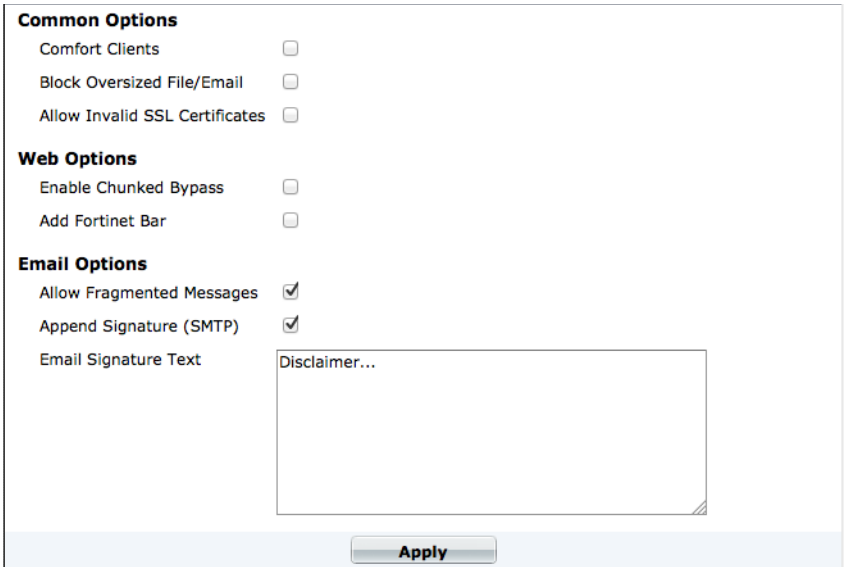
Common options, web options and email options

Here you can configure client comforting, whether to block oversized files or email, and whether or not to allow invalid SSL certificates.

Web options include enabling chunked by pass and adding the Fortinet bar (see “Fortinet Top Bar” on page 170).

Email options include allowing fragmented messages and appending a signature to all SMTP email messages.

Figure 77: Configuring common options, web options and email options



SSL and SSH inspection

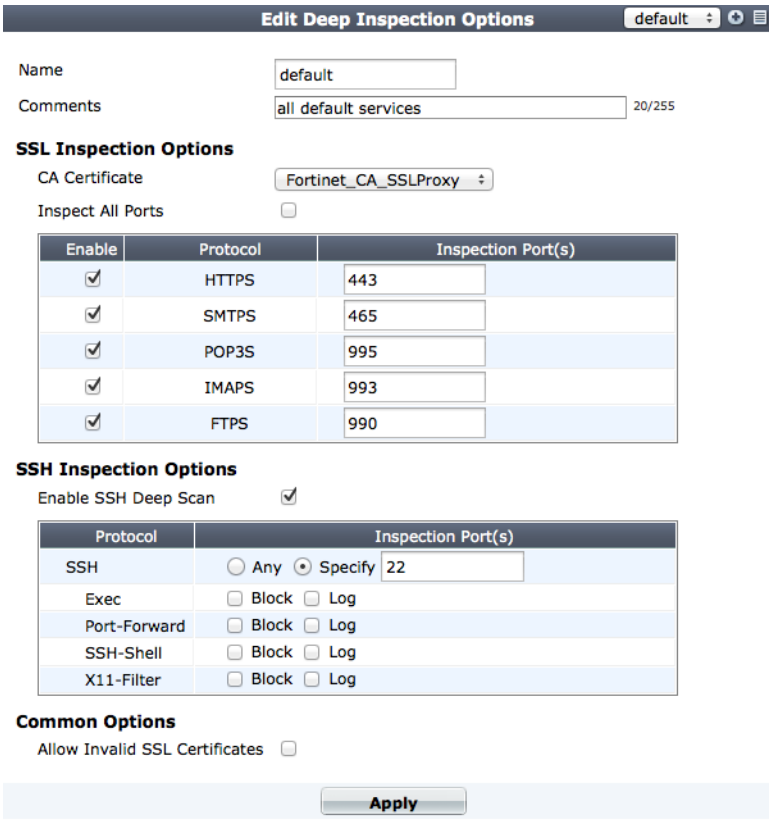
To configure how encrypted SSL or SSH traffic is inspected in security policy that accepts the SSL or SSH traffic to be inspected, turn on *SSL/SSH Inspection* and select an SSL/SSH inspection profile.

You can go to *Policy* > *Policy* > *SSL/SSH Inspection* to change the default SSL and SSH inspection profile or you can create new profiles.

SSL inspection options

For SSL traffic, you can select the certificate to use for this traffic and enable inspection of SSL traffic on all ports. You can also select individual SSL protocols and configure the inspection ports and port ranges for them. You can also choose to block or allow invalid SSL certificates.

Figure 78: Configuring SSL and SSH Inspection



SSH inspection options

For SSH traffic, you can enable SSH deep scanning, inspect all ports or specified ports for SSH traffic. You can also block or log all Exec, Port-Forward, SSH-Shell and X-11 SSH activity.

WAN optimization and Web Caching

In FortiOS 5.0, WAN optimization is enabled in security policies and WAN optimization rules are no longer required. Instead of adding a security policy that accepts traffic to be optimized and then creating WAN optimization rules to apply WAN optimization, in FortiOS 5.0 you create security policies that accept traffic to be optimized and enable WAN optimization in those policies. WAN optimization is applied by WAN optimization profiles which are created separately and added to the required security policies.

Because of this change, you can now apply all Security features to WAN optimization traffic without having to use a configuration that requires two VDOMS (one for applying Security features and one for applying WAN optimization). Instead, you can enable Security features in the security policies that accept WAN optimization traffic.

WAN optimization in policies requires you to add extra security policies with the incoming interface set to the new *wanopt* interface.

In FortiOS 4.3, you could create web caching only WAN optimization rules while in FortiOS 5.0 you cannot create web caching only WAN optimization profiles. Instead, you simply enable web caching in security policies, including WAN optimization policies. You can enable web caching for any WAN optimization policy. You can also enable HTTPS web caching and SSL offloading from the CLI for any security policy.

This chapter describes:

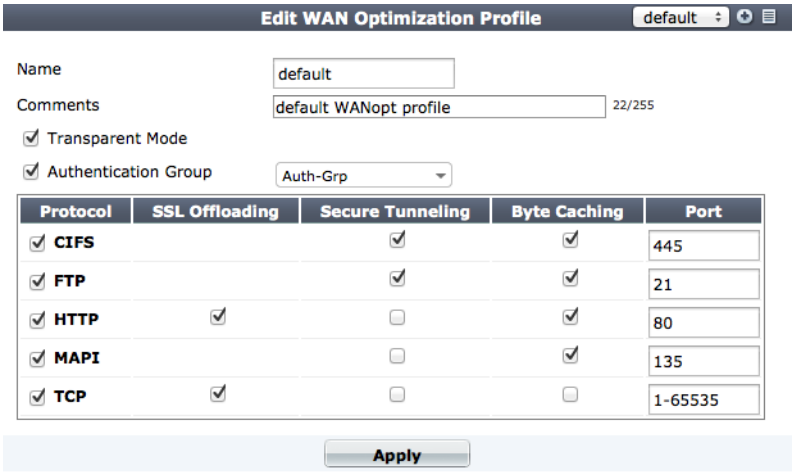
Configuring WAN optimization profiles

Use WAN optimization profiles to apply WAN optimization techniques to traffic to be optimized. In a WAN optimization profile, you can select the protocols to be optimized and for each protocol you can enable SSL offloading, secure tunneling, byte caching and set the port the protocol uses. You can also enable transparent mode and select an authentication group. You can edit the default WAN optimization profile or create new ones.

In order to configure WAN optimization profiles using the web-based manager, this feature must be enabled using Feature Select. For more information, see “Feature Select” on page 168.

To configure a WAN optimization profile go to *WAN Opt & Cache* > *WAN Opt. Profile* > *Profile* and edit a profile or create a new one.

Figure 79: Configuring a WAN optimization profile



From the CLI you can use the following command to configure a WAN optimization profile to optimize HTTP traffic.

```
config wanopt profile
  edit new-profile
    config http
      set status enable
  end
```

Enter the following command to view WAN optimization profile CLI options:

```
tree wanopt profile
-- [profile] --*name (36)
             |- transparent
             |- comments
             |- auth-group (36)
             |- <http> -- status
                       |- secure-tunnel
                       |- byte-caching
                       |- prefer-chunking
                       |- tunnel-sharing
                       |- log-traffic
                       |- port
                       |- ssl
                       |- ssl-port
                       |- unknown-http-version
                       +- tunnel-non-http
             |- <cifs> -- status
                       |- secure-tunnel
                       |- byte-caching
                       |- prefer-chunking
                       |- tunnel-sharing
                       |- log-traffic
                       +- port
             |- <mapi> -- status
                       |- secure-tunnel
                       |- byte-caching
                       |- tunnel-sharing
                       |- log-traffic
                       +- port
             |- <ftp> -- status
                      |- secure-tunnel
                      |- byte-caching
                      |- prefer-chunking
                      |- tunnel-sharing
                      |- log-traffic
                      +- port
             +- <tcp> -- status
                      |- secure-tunnel
                      |- byte-caching
                      |- byte-caching-opt
                      |- tunnel-sharing
                      |- log-traffic
                      |- port
                      |- ssl
                      +- ssl-port
```

Dynamic data chunking for WAN optimization byte caching

Dynamic data chunking helps to detect persistent data chunks in a changed files or in data embedded in traffic using an unknown protocol. For example, Lotus notes uses a private protocol to transfer email attachments in crafted messages. Dynamic data chunking performs byte caching of data in Lotus notes traffic. Dynamic data chunking is available for HTTP, CIFS and FTP.

Use the following command to enable dynamic data chunking for HTTP in the default WAN optimization profile.

```
config wanopt profile
  edit default
       config http
          set prefer-chunking dynamic
    end
```

By default, dynamic data chunking is disabled and `prefer-chunking` is set to `fix`.

Policy-based WAN optimization configuration changes summary

This section summarizes how basic WAN optimization configurations work in FortiOS 5.0, now that WAN optimization is enabled in security policies.

On the client side

New features:

- WAN optimization rules are removed and WAN optimization profiles are added. Profiles are configured in the client side.
- New options in firewall policies: `wanopt`, `wanopt-detection`, `wanopt-profile` and `wanopt-peer`. `wanopt-peer` is used only on the client side for manual mode (`wanopt-detection` is `off`).
- You can add Security features inspection to security policies that accept WAN optimization traffic.

On the server side

New features:

- New wanopt interface which represents the WAN optimization tunnel.
- Add a firewall policy with incoming (source) interface set to the wanopt interface to accept WAN optimization tunnel sessions (only required on the server side).
- For active/passive WAN optimization, set the server side to *passive*.
- For manual mode no WAN optimization policy required.
- WAN optimization profiles inherited by the server side.
- You can add Security feature inspection to security policies that accept WAN optimization traffic.

Client side configuration summary

WAN optimization profile

```
config wanopt profile
  edit "default"
    set comments "default WANopt profile"
      config http
        set status enable
        set prefer-chunking fix
    end
    config cifs
        set status enable
        set prefer-chunking fix
    end
        config mapi
        set status enable
    end
    config ftp
        set status enable
        set prefer-chunking fix
    end
    config tcp
        set status enable
        set byte-caching-opt mem-disk
    end
end
```

Local host ID and peer settings

```
config wanopt settings
  set host-id "client"
end
config wanopt peer
  edit "server"
  set ip 10.10.2.82
end
```

Security policies

Two client side WAN optimization security policy configurations are possible: one for active-passive WAN optimization and one for manual WAN optimization.

Active/passive mode on the client side

```
config firewall policy
  edit 2
    set srcintf "internal"
    set dstintf "wan1"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ANY"
    set utm-status enable <<< enable UTM
    set av-profile default <<< select an antivirus profile
    set profile-protocol-options default
    set wanopt enable <<< enable WAN optimization
    set wanopt-detection active <<< set the mode to active/passive
    set wanopt-profile "default" <<< select the wanopt profile
  next
end
```

Manual mode on the client side

```
config firewall policy
  edit 2
    set srcintf "internal"
    set dstintf "wan1"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ANY"
    set utm-status enable <<< enable UTM
    set av-profile default <<< select an antivirus profile
    set profile-protocol-options default
    set wanopt enable <<< enable WAN optimization
    set wanopt-detection off <<< sets the mode to manual
    set wanopt-profile "default" <<< select the wanopt profile
    set wanopt-peer "server" <<< set the only peer to do wanopt with
                                 (required for manual mode)
  next
end
```

Server Side configuration summary

Local host ID and peer settings

```
config wanopt settings
  set host-id "server"
end
config wanopt peer
  edit "client"
    set ip 10.10.2.81
end
```

Security policies

Two server side WAN optimization security policy configurations are possible: one for active-passive WAN optimization and one for manual WAN optimization.

Active/passive mode on server side

```
config firewall policy
   edit 2 <<< the passive mode policy
     set srcintf "wan1"
     set dstintf "internal"
     set srcaddr "all"
     set dstaddr "all"
     set action accept
     set schedule "always"
     set service "ANY"
     set utm-status enable <<< enable UTM
     set av-profile default <<< select an antivirus profile
     set profile-protocol-options default
     set wanopt enable
     set wanopt-detection passive
     set wanopt-passive-opt transparent
   next
   edit 3 <<< policy that accepts wanopt tunnel connections from the
             server
     set srcintf "wanopt" <<< wanopt tunnel interface
     set dstintf "internal"
     set srcaddr "all"
     set dstaddr "all"
     set action accept
     set schedule "always"
     set service "ANY"
   next
end
```

Manual mode on server side

```
configure firewall policy
  edit 3 <<< wanopt tunnel policy
    set srcintf "wanopt" <<< wanopt tunnel interface
    set dstintf "internal"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ANY"
    set utm-status enable <<< enable UTM
    set av-profile default <<< select an antivirus profile
    set profile-protocol-options default
  next
end
```

Combining web caching for HTTP traffic with WAN optimization

Web caching can be applied to any HTTP or HTTPS traffic by enabling web caching in a security policy that accepts the traffic. This includes WAN optimization and explicit web proxy traffic. Web caching caches all HTTP traffic accepted by a policy on TCP port 80.

You can add web caching to a WAN optimization security policy to combine web caching with WAN optimization for any WAN optimization security policy. This includes manual, active and passive WAN optimization policies and WAN optimization tunnel policies. You can enable web caching on both the client-side and the server-side FortiGate units or on just one or the other. For optimum performance, you can enable web caching on both the client-side and server-side FortiGate units. In this way, only uncached content is transmitted through the WAN optimization tunnel. All cached content is access locally by clients from the client side FortiGate unit.

Turning on web caching and SSL offloading for HTTPS traffic

Web caching can cache the content of HTTPS traffic on TCP port 443. With HTTPS web caching, the FortiGate unit receives the HTTPS traffic on behalf of the client, opens up the encrypted traffic and extracts content to be cached. Then FortiGate unit re-encrypts the traffic and sends it on to its intended recipient. It is very similar to a man-in-the-middle attack. You enable HTTPS web caching from the CLI in a security policy that accepts the traffic to be cached using `webcache-https`:

```
config firewall policy
  edit 0
    .
    .
    .
    set webcache enable
    set webcache-https any
    .
    .
    .
  end
```

The `any` setting causes the FortiGate unit to re-encrypt the traffic with the FortiGate unit's certificate rather than the original certificate. This configuration can cause errors for HTTPS clients because the name on the certificate does not match the name on the web site.

You can stop these errors from happening by configuring HTTPS web caching to use the web server's certificate by setting `webcache-https` to `ssl-server`:

```
config firewall policy
  edit 0
    .
    .
    .
    set webcache enable
    set webcache-https ssl-server
    .
    .
    .
  end
```

The `ssl-server` option causes the FortiGate unit to re-encrypt the traffic with the certificate that you imported into the FortiGate unit. The certificate is added to an SSL server configuration using the following command:

```
config wanopt ssl-server
  edit example_server
    set ip <Web-Server-IP>
    set port 443
    set ssl-mode { full | half}
    set ssl-cert <Web-Server-Cert>
  end
```

Where:

`Web-Server-IP` is the web server's IP address.

`Web-Server-Cert` is the original web server certificate imported into the FortiGate unit.

The SSL server configuration also determines whether the SSL server is operating in half or full mode and the port used for the HTTPS traffic.

Using the SSL server configuration, web caching also supports SSL offloading that uses the FortiGate unit's FortiASIC SSL encryption/decryption engine to accelerate SSL performance.

Changing the ports on which to look for HTTP and HTTPS traffic to cache

By default, FortiOS assumes HTTP traffic uses TCP port 80 and HTTPS traffic uses port 443 and so web caching is configured for all HTTP traffic accepted by a policy on TCP port 80 and all HTTPS traffic on TCP port 443. If you want to cache HTTP or HTTPS traffic on other ports, you can enable Security features for the security policy and add an SSL/SSH inspection profile that looks for HTTP and HTTPS traffic on other TCP ports.

Setting the HTTP port to *Any* in the an SSL/SSH inspection profile is not compatible with web caching. If you set the HTTP port to any, web caching only caches HTTP traffic on port 80.

Web proxy URL debugging

You can use the following CLI commands to get debugging information that shows how the web cache is handling specific URLs. You can debug web caching for a single web page (such as docs.fortinet.com/fgt40mr3.html) or for all requests to a URL pattern (such as docs.fortinet.com to debug all connections to any page on docs.fortinet.com). Wildcard characters and regular expressions are not supported.

Normally you would use this feature if the web cache was not caching specific pages and sites. It makes it easier to get debug information just for the pages causing the problem. This feature works for web caching enabled in any security policy including web proxy and WAN optimization security policies.

Debugging caching of a specific web page

Start by adding the URL to the configuration:

```
config web-proxy debug-url
  edit docs-url
    set url-pattern "docs.fortinet.com/fgt40mr3.html"
    set status enable
    set exact enable
  end
```

Then enter the following commands to enable debugging:

```
diagnose debug application wad 0
diagnose wad debug-url enable
diagnose debug enable
```

The CLI then displays debug information as the `wad` application processes sessions. However, the `diagnose wad debug-url enable` command isolates and formats the debug output for sessions to and from docs.fortinet.cm/fgt40mr3.html.

Example output when a user browses to docs.fortinet.cm/fgt40mr3.html with Firefox. You may have to scroll through other debug output to find this, but its should be easy to find because its formatted differently than the other web cache diagnose output.

```
[0x40d977d0] Received request from client: 10.31.101.20:54932

GET /fgt40mr3.html HTTP/1.1
Host: docs.fortinet.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:5.0.1)
     Gecko/20100101 Firefox/5.0.1
Accept:
     text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
DNT: 1
Connection: keep-alive
Referer: http://docs.fortinet.com/fgt.html

[0x40d977d0] Connect to server: 208.91.113.43:80

[0x40d977d0] Forward request to server:
```

```
GET /fgt40mr3.html HTTP/1.1
Host: docs.fortinet.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:5.0.1)
     Gecko/20100101 Firefox/5.0.1
Accept:
     text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
DNT: 1
Referer: http://docs.fortinet.com/fgt.html
Connection: Keep-Alive

[0x40d977d0] Received response from server:

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Fri, 10 Feb 2012 17:05:15 GMT
X-Powered-By: ASP.NET
Connection: close
Content-Type: text/html

[0x40d977d0] Forward response from sever:

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Fri, 10 Feb 2012 17:05:15 GMT
X-Powered-By: ASP.NET
Content-Type: text/html
Connection: close
```

Debugging caching of multiple web pages

Use the following commands to get URL debugging output when any docs.fortinet.com and www.fortinet.com web page is cached. In this configuration, just the high-level URLs are added to the configuration and `exact` is set to disable:

```
config web-proxy debug-url
  edit docs-url
    set url-pattern “docs.fortinet.com”
    set status enable
    set exact disable
  next
  edit docs-url
    set url-pattern “www.fortinet.com”
    set status enable
    set exact disable
  next
end
```

Then enter the following commands to enable debugging:

```
diagnose debug application wad 0
diagnose wad debug-url enable
diagnose debug enable
```

The CLI then displays debug information as the `wad` application processes sessions, highlighting all connections to docs.fortinet.com and www.fortinet.com.

FortiOS Web Caching now caches Windows/MS-Office software updates

FortiOS web caching is not always able to cache Windows and MS-Office updates because they are downloaded using HTTP in multipart or chunked mode and typically run through multiple TCP connections. To resolve this issue in FortiOS 5.0, the first request for Windows or MS-Office updates (to download.windowsupdate.com) causes the cache process to download the new update file in the background.

Once the new update file has been downloaded to the cache, it is available to web cache users and all subsequent requests for this update will be downloaded from the cache. Because the update file will not be available in the web cache until it has completely downloaded, the first update request will not be able to get it from the web cache and neither will any updates requested while the file is downloading in the background.

Usability enhancements

FortiOS 5.0 introduces usability enhancements to make configuration easier and management more effective and efficient.

New usability features include:

- Feature Select
- Improved list editing
- Dynamic comment fields
- Setup Wizard enhancements
- Fortinet Top Bar
- VDOM Mode GUI changes
- Enhanced Top Sessions dashboard widget
- Improved CLI syntax for multi-value fields

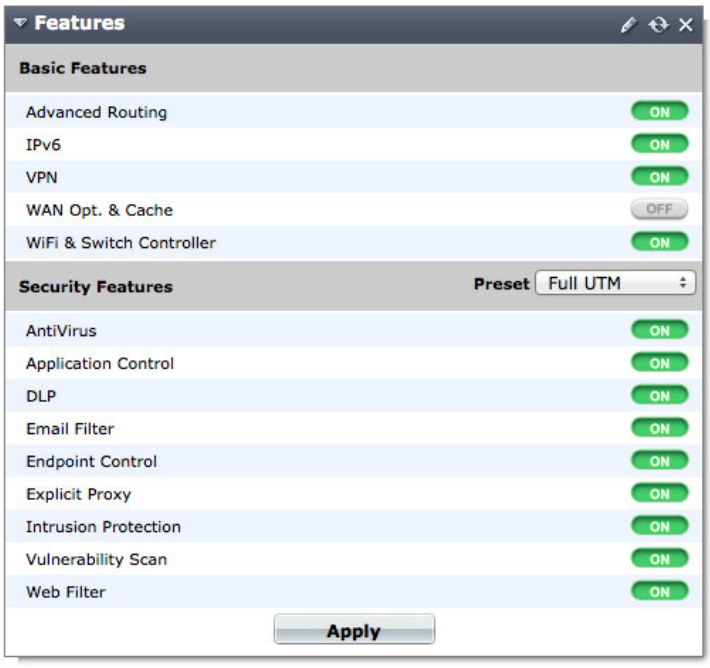
Feature Select

Feature Select is used to disable features which are not required for network administration. Disabling features also removes all related configuration options from the web-based manager.

This feature replaces the previous GUI display options control.

Feature Select can be managed using the *Features* widget on the *Status* page. They can also be found at *System* > *Config* > *Features*, where additional features are also available by selecting *Show More*.

Figure 80: The Features widget



Security Features Presets

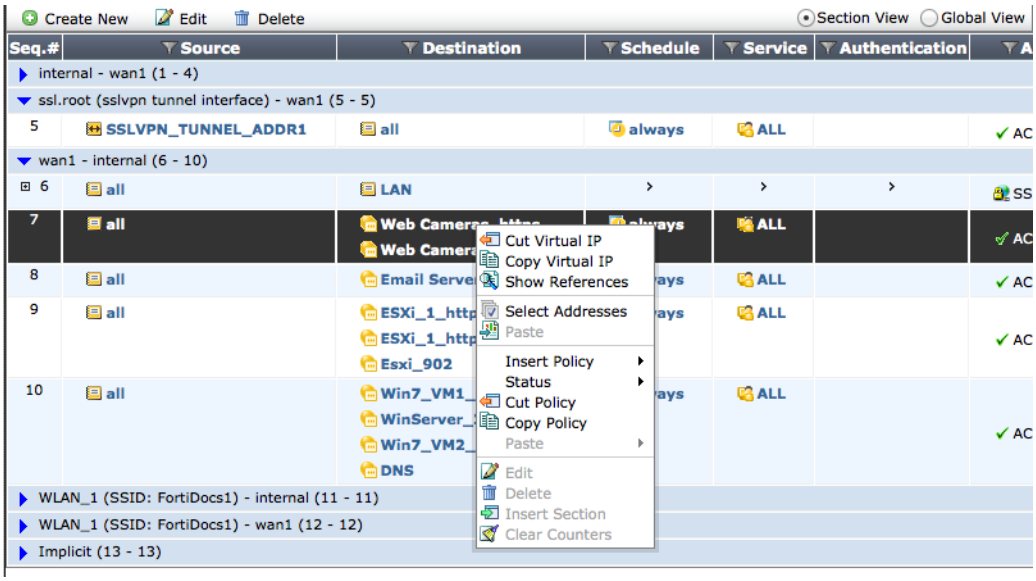
The main Security Features can be turned off individually or the five system presets can be used:

- *UTM* should be chosen for networks that require full protection from FortiOS. UTM is the default setting.
- *WF* should be chosen for networks that require web filtering.
- *ATP* should be chosen for networks that require protection from viruses and other external threats.
- *NGFW* should be chosen for networks that require application control and protection from external attacks.
- *NGFW + ATP* should be chosen for networks that require protection from external threats and attacks.

Improved list editing

List editing has been enhanced on most lists of configuration items on the FortiOS 5.0 web-based manager. On most list items, you can click on any item to display a list of options. The options available depend on the item and context.

Figure 81: Example security policy list address menu



Dynamic comment fields

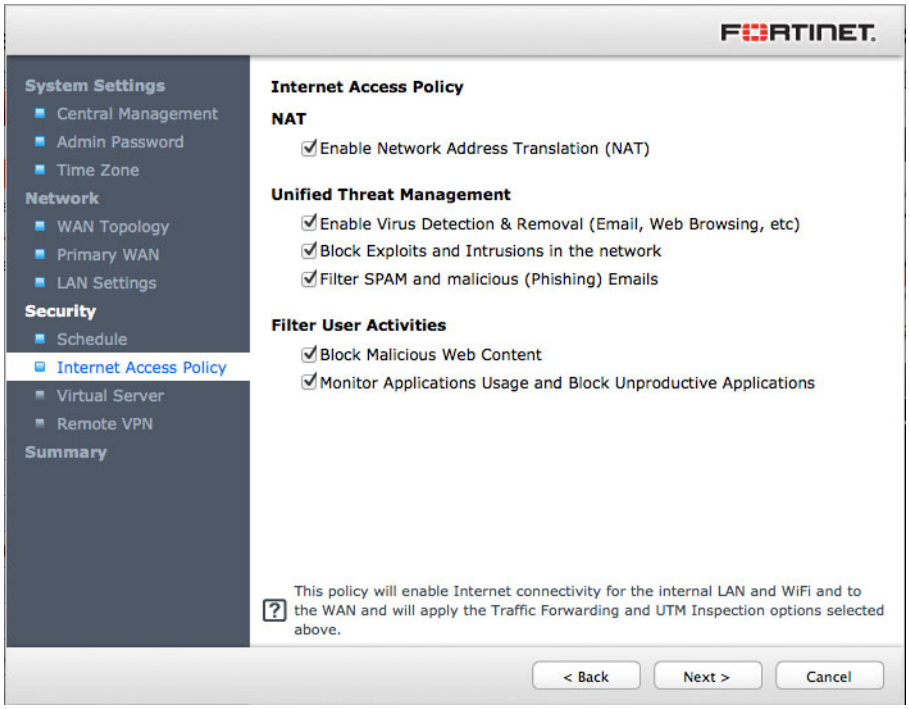
Most comment fields available from the web-based manager and CLI have been extended to a maximum of 255 characters and others to a maximum of 1023 characters. To save system memory, the amount of storage space for comment fields is dynamically allocated based on the size of the comment.

Setup Wizard enhancements

The Setup Wizard is now available for all FortiGate units. On individual models the wizard can include advanced or model-specific configuration options, such as load balancing, 3G/4G modem, virtual servers, remote VPN and the opportunity to configure all available interfaces.

The Setup Wizard also allows you to enable central management. When this option is selected, much of the Wizard is bypassed because a FortiManager unit supplies the configuration information. The WAN Topology and Primary WAN wizard pages are still presented for configuration because the FortiGate unit must be able to connect to its network before FortiManager can contact it.

Figure 82: Setup wizard - Internet access policy setup



Fortinet Top Bar

You can configure the FortiGate unit to overlay a Fortinet status bar on your user's web pages by going to *Policy* > *Policy* > *Proxy Options* and selecting *Add Fortinet Bar* and then by adding this Proxy Options profile to a security policy. Whenever a user accesses a web page through this policy, the Fortinet Top Bar is displayed overlaying the upper right corder of the web page.

The top bar can display a user ID if the user has authenticated with the FortiGate unit (in the example the user ID is bdickie). You can select the user icon to sign out of the FortiGate unit.

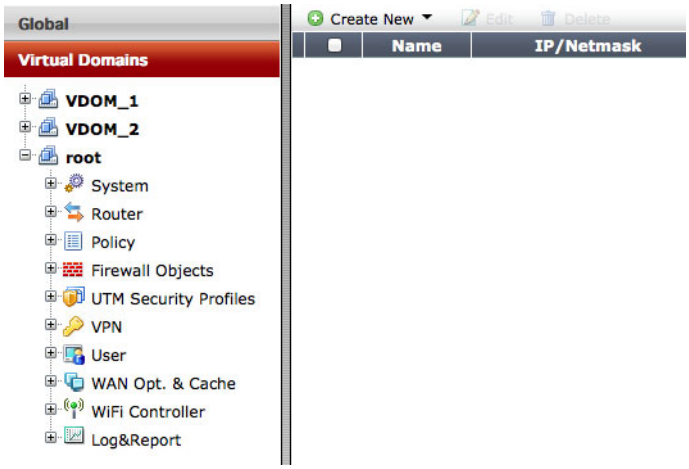
The top bar can also display other information such as:

- Application control violations
- Endpoint control enforcement
- Your web browsing quota
- User ID if the user has authenticated
- SSL VPN status and bookmarks

VDOM Mode GUI changes

When operating a FortiGate unit with VDOMs enabled, when you log in as a system administrator who can access multiple VDOMs, the VDOMs you can access appear under Virtual Domains in the left web-based manager menu. Figure 83 shows an example VDOM menu for a FortiGate unit with three virtual domains.

Figure 83:VDOM menu



Enhanced Top Sessions dashboard widget

The Top Sessions dashboard widget has been enhanced to allow you to display information about sessions according to their source address, destination address and the application creating the sessions. To demonstrate this new functionality, by default the web-based manager includes three new dashboards.

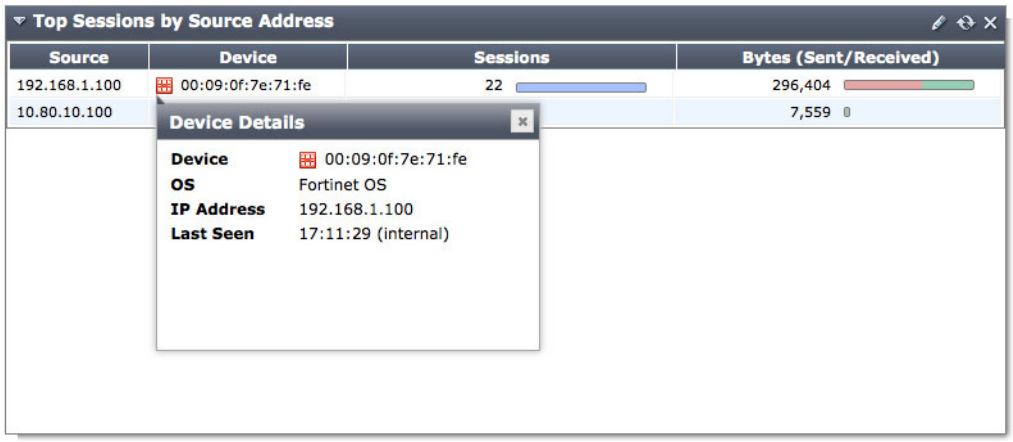
You may need to reset your dashboard if these dashboard widgets are not appearing. To reset the dashboard, select *Reset Dashboards* from the *Dashboard* menu.

Top Sources

Top sources displays the top 25 source addresses. For each source address, the widget displays device information, host name, the number of active sessions and the amount of data sent/received by the device. You can hover over the device icon to get more information about

the device. You can also select an entry to see all of the individual sessions from that source address. The session table includes the destination address, security policy, application name and amount of data sent and received by the session.

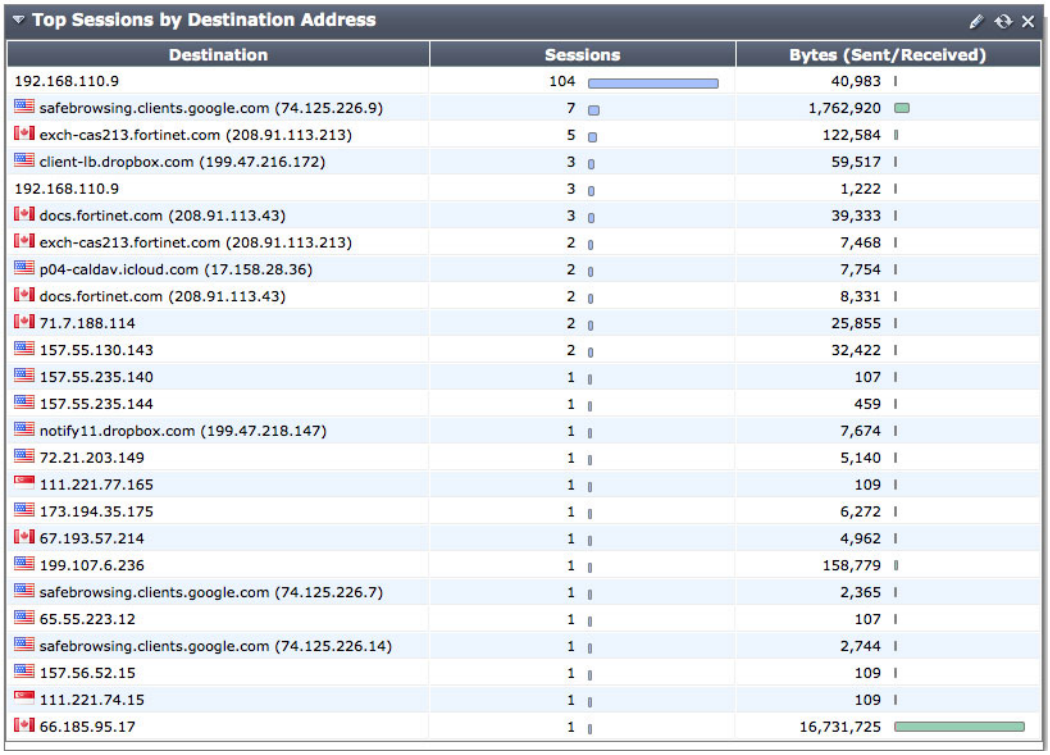
Figure 84: Top Sessions by Source Address



Top Destinations

Top destinations displays the top 25 destination addresses. For each destination address, the widget displays the destination host name and country, the number of sessions going to the destination and the amount of data in bytes sent and received by the destination. You can select an entry to see the individual sessions to that destination address. The session table includes the source address, security policy, application name and amount of data sent received by the session.

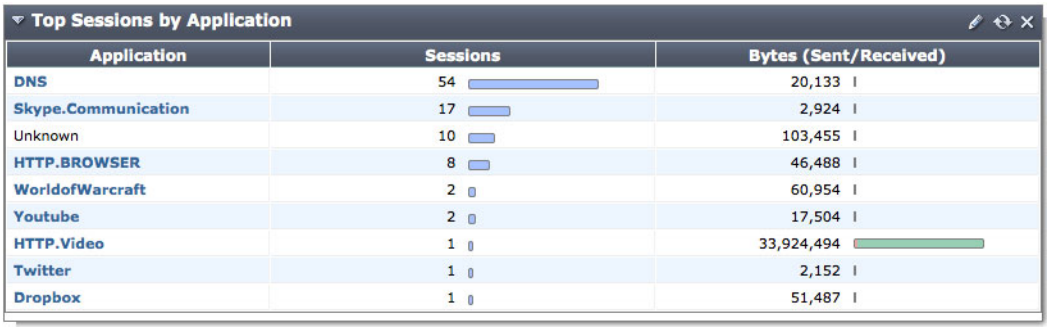
Figure 85: Top Sessions by Destination Address



Top Applications

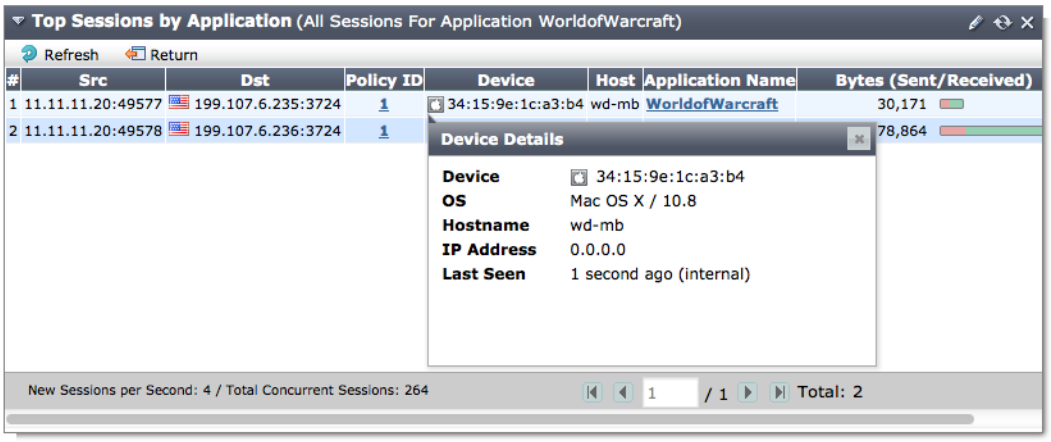
Top applications displays the top 25 applications sending traffic through the FortiGate unit. For this widget to show data, you must enable application control for security policies that allow traffic through the FortiGate unit.

Figure 86: Top Sessions by Application



For each application, the widget displays the application name, the number of sessions and the amount of data in bytes sent and received. You can select the application name to get more information about the application. You can select an entry to see the individual sessions for that application. The session table includes the source address, destination address, security policy, application name and amount of data sent received by the session.

Figure 87: Details about the sessions for an application



Identifying Skype sessions

If Skype is in use on your network, Skype sessions may appear on the *Top Sessions By Application* list with the *Application Name* displayed as *unknown*. You can help the FortiGate unit identify Skype sessions by using the following command to add the public IP address of your network to the FortiGate configuration.

For example, if the IP address of the FortiGate interface connected to the Internet is 172.20.120.14 and if the security policies for connections to the Internet have source NAT enabled, enter the following command to add the public IP address of your network which is the public address used by Skype sessions:

```
config ips global
  set skype-client-public-ipaddr 172.20.120.14
end
```

You can add multiple IP addresses with this command. This can be useful if your network or your Skype sessions have more than one public IP address. For example, you may have multiple Internet connections each with a different IP address. Also, if the external IP address is set using DHCP or PPPoE it may change and you can add multiple IP addresses to help account for this. Use the following command to add multiple public IP addresses (separate the addresses with a comma and no spaces).

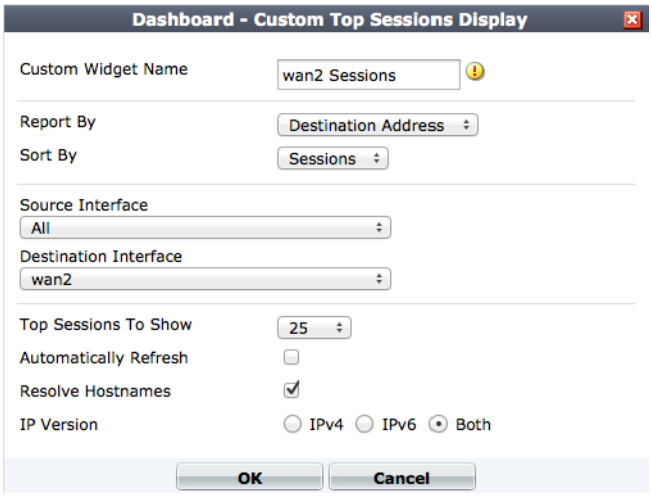
```
config ips global
  set skype-client-public-ipaddr 172.20.120.14,10.10.10.20
end
```

You may not have direct knowledge of your network's public IP address. This can happen for a number of reasons, depending on your network configuration. For example, your FortiGate unit may not be connected directly to the Internet. To make sure you are adding the right IP addresses you can use free services such as WhatIsMyIP.com to verify your network's public IP address.

Customizing the Top Sessions dashboard widget

You can create multiple top sessions dashboard widgets that report sessions by source address, destination address or application. You can customize the widgets with a custom widget name, control the source and destination interfaces of the sessions and determine whether to sort the sessions by bytes or by number of sessions.

Figure 88: Customizing the Top Sessions dashboard widget



Improved CLI syntax for multi-value fields

Several new subcommands simplify editing of CLI fields that accept multiple values. This eliminates re-typing of lists of options, IP addresses, and so on, saving time and avoiding errors. You can simply add or remove individual items from the list.

Table 3: CLI subcommands for multi-value fields

`append <field_name> <list>`	Add one or more values to the list.
`unselect <field_name> <list>`	Remove one or more values from the list.

`select <field_name> <list>`	Select one or more values. This is the same as the `set` subcommand.
`clear <field_name>`	Reset the multi-value field to its default value. This is the same as the `unset` subcommand.

You can continue to use the `set` and `unset` subcommands on multi-value fields.

The new subcommands support command completion. For example, in the `config system interface` command, if you enter select ?, the response shows only the multi-value fields:

```
dhcp-relay-ip    dhcp relay ip address
allowaccess      Allow management access to the interface
```

Example

Prior to FortiOS 5.0, to add SSH administrative access to an interface that currently allows HTTPS, FGFM and PING access, you would enter:

```
set allowaccess https fgfm ping ssh
```

In FortiOS 5.0, you can do this:

```
append allowaccess ssh
```

Similarly, to remove `ping` from the list, you would enter:

```
unselect allowaccess ping
```

To reset `allowaccess` to its default, you would enter:

```
clear allowaccess
```

SSL VPN

New SSL VPN features include:

New default SSL VPN portals

FortiOS 5.0 includes 3 new default SSL VPN portal configurations:

- full-access is a general use portal that includes tunnel mode and web mode and supports all possible supported applications over the SSL VPN. Split tunneling and including the FortiClient download is not enabled.
- tunnel-access only includes support for tunnel mode (and not web mode). Split tunneling is enabled and remote users are prompted to download FortiClient.
- web-access only includes support for web mode. The connection tool and FortiClient download options are disabled.

SSL VPN user groups no longer required

The distinction between SSL VPN user groups and firewall user groups has been removed. Any use group can be used for SSL VPN authentication, except FSSO user groups.

SSL VPN policy interface name change

The former SSL.root interface used in SSL VPN security policies as the source or destination interface for SSL VPN traffic has been renamed to *sslvpn tunnel interface*.

Support SSL VPN push configuration of DNS suffix

You can now assign one or more DNS suffixes to the FortiGate SSL VPN configuration so that SSL VPN clients do not need to use full-qualified host names to connect to internal resources. If you add one suffix, it is always attached to DNS queries.

If you add more than one suffix the FortiGate unit will attempt a DNS lookup by adding each suffix and use the first one that can be found in the DNS database. Multiple suffixes should be added in the proper search order. You can use up to 253 characters to add one or more DNS suffixes. Separate the suffixes with a space.

For example, if an organization requires DNS suffixes for example.com and example.org and you want DNS queries to try example.com first, you can use the following command to add these suffixes to the SSL VPN configuration:

Use the following command to add a DNS suffix that is used for SSL VPN sessions:

```
config vpn ssl settings
  set dns-suffix ”example.com example.org”
end
```

Other new features

This chapter provides a brief introduction to the following new features:

New FortiGuard features

The following FortiGuard services are available for any FortiGate unit free of charge:

- System time from FortiGuard NTP servers
- Default DNS configuration uses FortiGuard DNS servers

With a valid support contract, the following FortiGuard services are also available:

- Antivirus database updates
- IPS signature updates
- Vulnerability scan signature updates
- FortiGuard Web Filtering lookups
  - DNS-based Web Filtering; the FortiGuard DNS server network returns web filter ratings. DNS web filtering uses less CPU time, system memory and network bandwidth than proxy or flow-based FortiGuard web filtering, resulting in better performance.
  - IP address reputation scores from the FortiGuard DNS server network.
- FortiGuard Email filtering lookups
- Geographic address database for geographic firewall addressing
- BYOD device signature updates
- USB Modem Updates

FortiGate Auto-config using DHCP

FortiOS 5.0 supports uploading a configuration file from a TFTP server to the FortiGate unit to automatically configure the FortiGate unit with one simple step. Similar to an auto-configuration feature used for VoIP phones, you can store the domain name or IP address of a TFTP server and a configuration file name in your DHCP server configuration.

- DHCP option 66 is used for the TFTP server domain name (RFC 2132)
- DHCP option 67 is used for the configuration file name (RFC 2132)

For example, to use auto-configuration to configure a FortiGate unit, add the TFTP server information and configuration file name to your DHCP server. Make sure the TFTP server is running and includes the configuration file. Then, from the CLI of the FortiGate unit to be auto-configured, enter the following command (assuming the FortiGate internal interface is connected to the same network as the TFTP server).

```
execute restore config dhcp internal
```

The FortiGate unit gets the information it needs from the DHCP server, downloads and installs the configuration file from the TFTP server and restarts running its new configuration.

If the TFTP server is only available on a VLAN network (for example, VLAN id 224), you can use the following command to access the TFTP server on the VLAN network:

```
execute restore config dhcp internal 224
```

FortiGate Session Life Support Protocol (FGSP)

In a network that already includes load balancing (either with load balancers or routers) for traffic redundancy, two FortiGate units can be integrated into the load balancing configuration using the FortiGate Session Life Support Protocol (FGSP). The external load balancers or routers can distribute IPv4 and IPv6 TCP, UDP, ICMP and expectation, and NAT sessions among the FortiGate units and the FGSP performs ***session synchronization*** to keep the session tables of both FortiGate units synchronized.

If one of the FortiGate units fails, session failover occurs and active sessions fail over to the unit that is still operating. This failover occurs without any loss of data. As well, the external load balancers or routers detect the failover and re-distribute all sessions to the unit that is still operating.

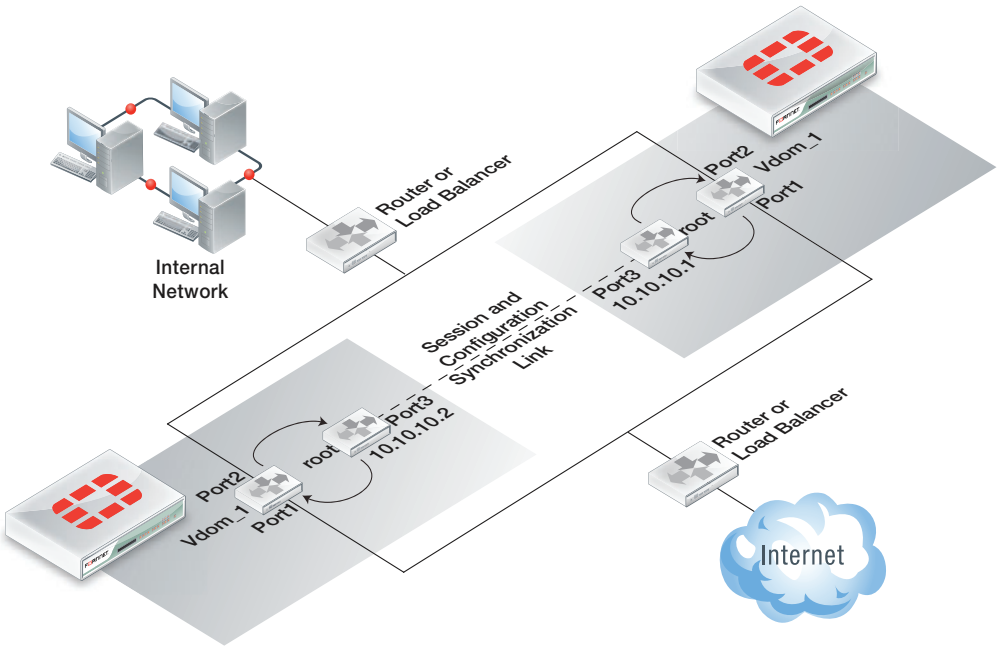
Load balancing and session failover is done by external routers or load balancers and not by the FGSP. The FortiGate units perform session synchronization which allows session failover to occur without packet loss.

The FGSP also includes ***configuration synchronization***, allowing you to make configuration changes at once for both FortiGate units, instead of requiring duplicate configuration changes on each unit.

Settings that identify the FortiGate unit to the network, for example, interface IP addresses and BGP neighbor settings, are not synchronized so that each FortiGate unit maintains its identity on the network. These settings must be configured separately for each FortiGate unit.

In previous versions of FortiOS, the FGSP was called TCP session synchronization or standalone session synchronization. However, the FGSP has been expanded to include configuration synchronization and session synchronization of connectionless sessions, expectation sessions, and NAT sessions.

Figure 89: Example FGSP HA configuration



HA failover supports more features

FortiOS 5.0 HA and the FortiGate Clustering Protocol (FGCP) support the following new types of failover:

- IPv6 session failover: if session pickup is enabled, IPv6 sessions are synchronized between cluster members and, after an HA failover, IPv6 sessions will resume with only minimal interruption.
- NAT64 session failover: if session pickup is enabled, NAT64 sessions are synchronized between cluster members and, after an HA failover, NAT64 sessions will resume with only minimal interruption.
- Full support for NAT 66 session failover: if session pickup is enabled, after an HA failover, NAT66 sessions will resume with only minimal interruption.
- SSL VPN authentication failover support: if session pick is enabled, SSL VPN sessions will resume after a failover without requiring SSL VPN users to re-authenticate.
- Device identification and management (BYOD).

New HA mode: Fortinet redundant UTM protocol (FRUP)

FortiOS 5.0 includes an extension to the FotiGate Clustering Protocol that combines Switching HA and Firewall HA into a single unified design. This feature is initially available on the FortiGate-100D and will be considered for other models in future releases.

A FRUPS setup consists of 2 (and only 2) identical FortiGate-100D units. The setup supports dual redundant HA links between the units for sharing session and configuration data.

To see a FRUP example, please refer to Cookbook Beta - FortiGate Redundant UTM Protocol.

ICAP and the explicit web proxy

Internet Content Adaptation Protocol (ICAP) profiles can be added to explicit web proxy security policies. ICAP is a light-weight response/request protocol that allows the FortiGate unit to offload explicit web proxy traffic to external servers for different kinds of processing. ICAP is often used for offloading virus scanning and web filtering but has many other applications.

If you enable ICAP in a web proxy security policy, HTTP traffic intercepted by the explicit web proxy is transferred to an ICAP server in the ICAP profile added to the policy. Responses from the ICAP server are returned to the FortiGate unit which forwards them to their destination.

You can offload HTTP responses or HTTP requests (or both) to the same or different ICAP servers. You can also enable streaming media bypass.

Example ICAP sequence for an ICAP server performing web URL filtering on web proxy HTTP requests

1 A user opens a web browser and sends an HTTP request to connect to a web server.

2 The FortiGate unit intercepts the HTTP request and forwards it to an ICAP server.

3 The ICAP server receives the request and determines if the request is for URL that should be blocked or allowed.

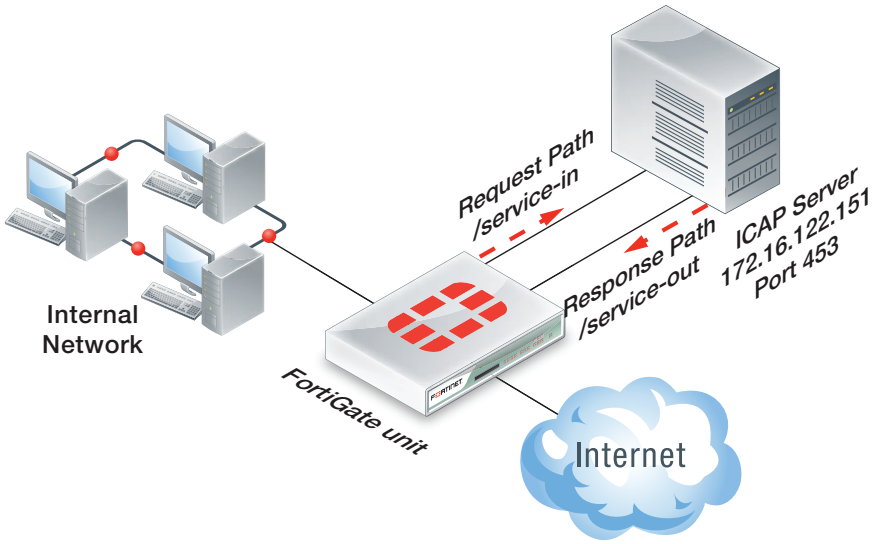
- If the URL should be blocked, the ICAP server sends a response to the FortiGate unit. The FortiGate unit returns this response to the user's web browser. This response could be a message informing the user that their request was blocked.
- If the URL should be allowed, the ICAP server sends a request to the FortiGate unit. The FortiGate unit forwards the request to the web server that the user originally attempted to connect to.

When configuring ICAP on the FortiGate unit, you must configure an ICAP profile that contains the ICAP server information; this profile is then applied to a security policy.

Example ICAP configuration

The following example shows how to configure the FortiGate unit to offload processing to an ICAP server. The ICAP server IP address is 172.16.122.151 and port it is listening on is 453. The ICAP server request path /service-in and its response path is /service-out.

Figure 90: Example ICAP network configuration



Adding ICAP to a web proxy security policy - web-based manager

In order to configure ICAP using the web-based manager, this feature must be enabled using Feature Select. For more information, see “Feature Select” on page 168.

The following is an example of configuring the ICAP feature on the FortiGate unit and applying an ICAP profile to an existing web proxy security policy.

1 Go to *Security Profiles* > *ICAP* > *Servers* and select *Create New* to add the following ICAP server:

Name	New ICAP Server
IP Type	IPv4
IP Address	172.16.122.151
Port	453

2 Go to *Security Profiles* > *ICAP* > *Profiles* and select *Create New* to add an ICAP profile names *New ICAP Profile.*

3 Select *Enable Request Processing* and configure the following:

Server	New ICAP Server
Path	/service-in
On Failure	Error

4 Select *Enable Response Processing* and configure the following:

Server	New ICAP Server
Path	/service-out
On Failure	Error

5 Select *Enable Streaming Media Bypass* and select *OK*.

6 Go to *Policy* > *Policy* > *Policy* and edit the security policy that accepts the traffic to be processed by the ICAP server.

7 Under *Security Policies*, select *Enable ICAP* and set *New ICAP Server*.

8 Select *OK*.

Adding ICAP to a web proxy security policy - CLI

The following is an example of configuring the ICAP feature on the FortiGate unit and applying an ICAP profile to an existing web proxy security policy.

1 Log in to the CLI.

2 Enter the following to configure the ICAP server:

```
config icap server
  edit “New ICAP Server”
    set ip-address 172.16.122.151
    set ip-version 4
    set max-connections 100
    set port 453
  end
```

3 Enter the following to configure the ICAP profile to then apply to a security policy:

```
config icap profile
  edit "New ICAP Profile"
    set request enable
    set request-failure error
    set request-path "/service-in"
    set request-server icap_server
    set response enable
    set response-failure error
    set response-path "/service-out"
    set response-server "New ICAP Server"
    set streaming-content-bypass enable
  end
```

4 In the `config firewall policy` command, apply the ICAP profile to a security policy:

```
config firewall policy
  edit 0
    set srcintf web-proxy
    ...
    set utm-status enable
    set icap-profile "New ICAP Profile"
  end
```

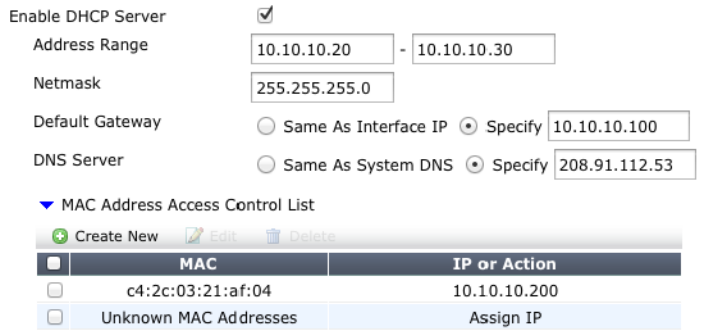
New interface features - DHCP server and authentication

You can add a DHCP server and authentication to any FortiGate interface. This includes physical interfaces, WiFi interfaces (SSIDs), switch interfaces (software and hardware switch interfaces), aggregate interfaces, redundant interfaces, loopback interfaces and VLAN interfaces.

Adding a DHCP server to an interface

To add a DHCP server to an interface, edit the interface and select *Enable DHCP Server*. Then you can specify the address range, netmask, default gateway and DNS servers provided by the DHCP server. An interface must have a static IP address to add a DHCP server to it.

Figure 91: Adding a DHCP server to a FortiGate interface

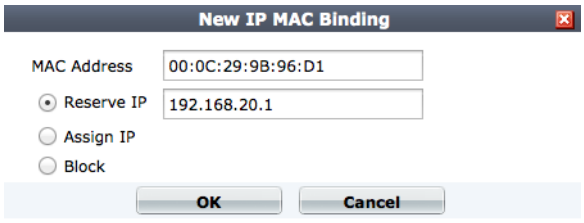


Reserving, assigning and blocking MAC addresses

While adding a DHCP server to an interface you can select *MAC Address Control list* and select *Create New* to configure the DHCP server to:

- Always assign the same IP address to a device according to its MAC address (*Reserved IP* address)
- *Block* access to a device according to its MAC address (MAC address filtering)
- The default action is to *Assign* an IP address to a device.

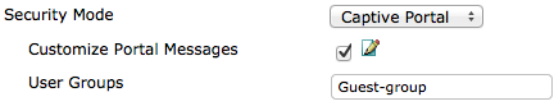
Figure 92: Reserving an IP address for a device with a specific MAC address



Authentication - Captive Portal

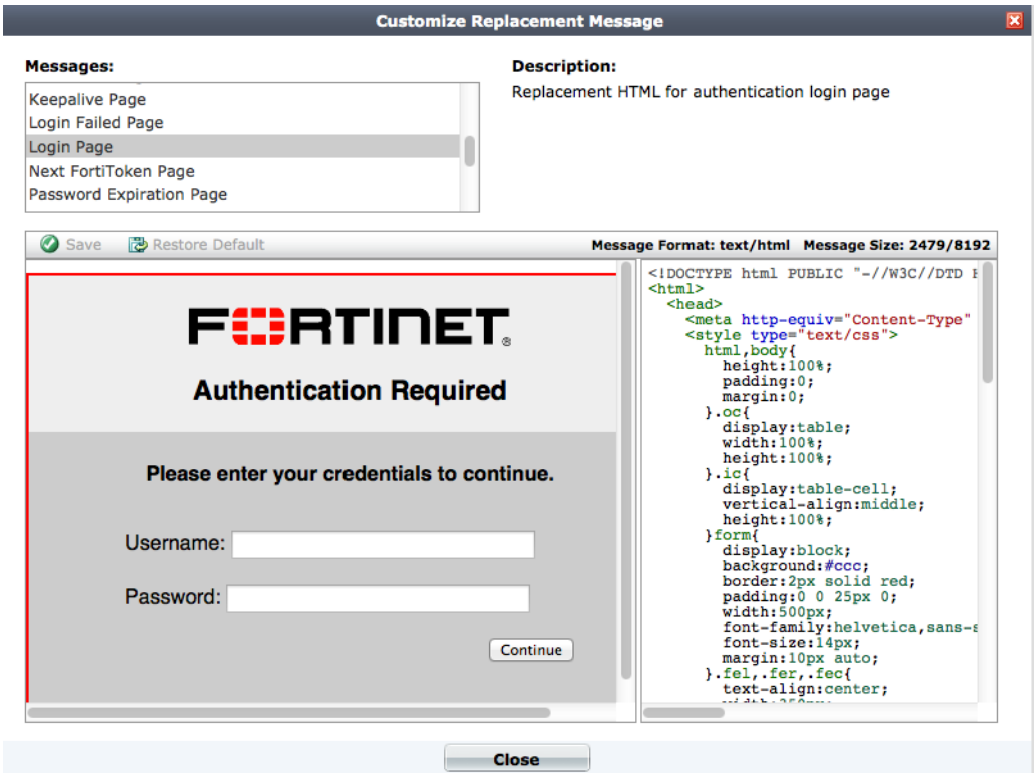
To add authentication to an interface, edit an interface and set *Security Mode* to *Captive Portal*. Then select one or more *User Groups*. Users who attempt to connect through the interface must first use HTTP or HTTPS to connect to a captive portal and enter a user name and password.

Figure 93: Reserving an IP address for a device with a specific MAC address



You can customize the captive portal for each interface or select from a saved portal.

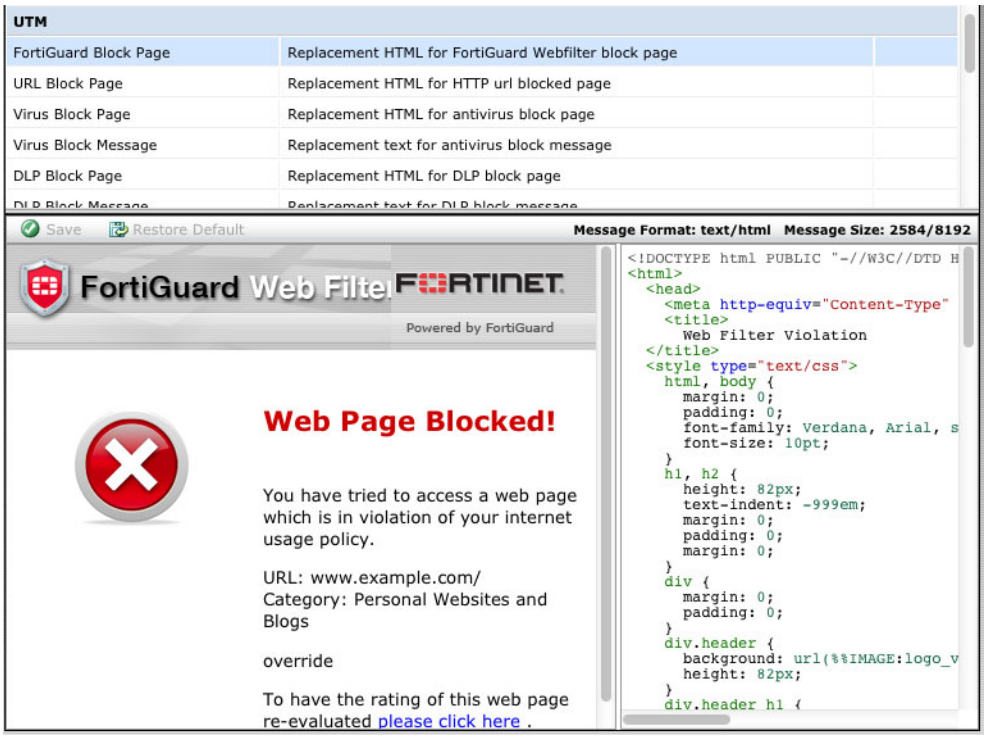
Figure 94: Customizing the captive portal



Replacement Message Improvements

Go to *System* > *Config* > *Replacement Messages* to edit replacement messages. Editing replacement messages has been enhanced with a new editor that you can use to select and edit replacement messages and view your changes in real time as you make them.

Figure 95: Editing replacement messages



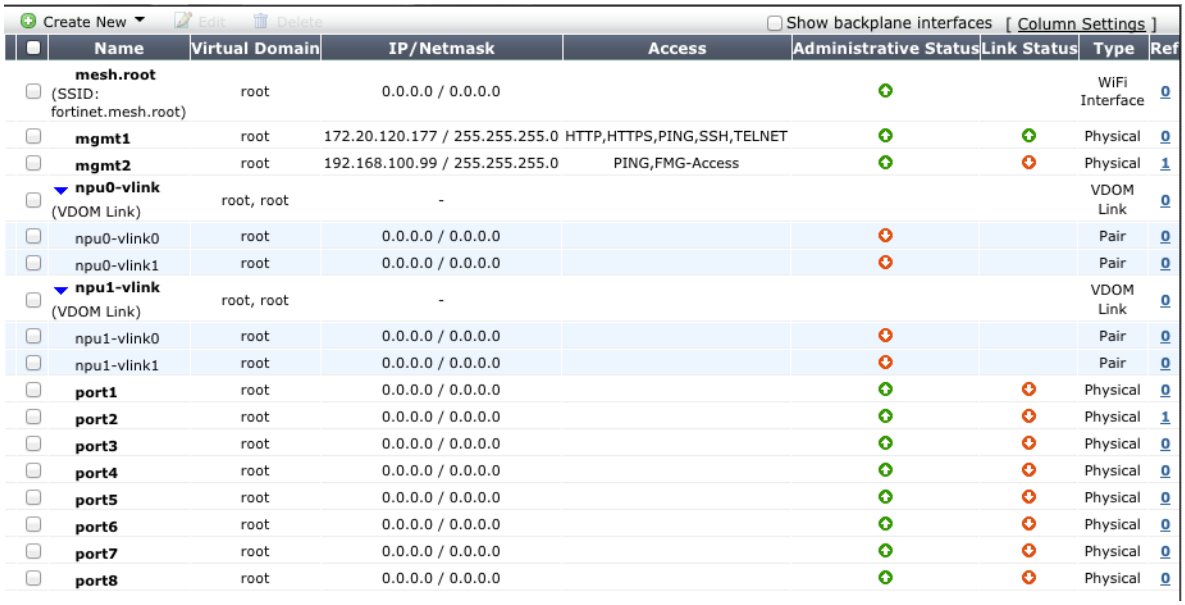
In addition, more replacement messages are available and the replacement message editor includes simple and extended view. The simple view includes the most commonly edited replacement messages while the extended view includes all of them.

Acceleration of Inter-VDOM Traffic (by NP4)

On high-end FortiGate units that include NP4 processors, you can add inter-VDOM links where the traffic is accelerated by NP4 processors. This means enhanced performance for traffic passing between VDOMs that will improve the overall performance and capacity of many multiple VDOM implementations.

If your FortiGate unit supports accelerated inter-VDOM links, when it is operating in multiple VDOM mode, the interface list includes interfaces with names such as npu0-vlink0, npu1-vlink and so on (see Figure 96).

Figure 96: FortiGate-5001B interface list showing NP4 accelerated inter-VDOM links



By default, all of these links are associated with the root VDOM. However, you can edit each interface in the link and add it another VDOM, creating an inter-VDOM link between 2 VDOMs

Virtual Hardware Switch

In previous versions of FortiOS, you can use the software switch feature to group independent interfaces into a single logical switch. In this virtual software switch, all of the interfaces share the same IP address and be connected to the same subnet and traffic would pass between them as if they were switch ports, with no firewall or other FortiGate features applied to the traffic. However, the virtual software switch feature just simulates a switch and, since the FortiGate CPU must process the switch traffic, performance can be affected if the FortiGate unit becomes busy processing a lot of traffic.

In FortiOS 5.0, for FortiGate models that have internal hardware switches, you can use the following command to group interfaces in the hardware switch into virtual hardware switches in which all traffic between the switch ports is processed on the switch itself and the FortiGate CPU is not involved resulting in improved performance.

Recent FortiGate models with internal hardware switches support this feature.

Use the following command to create a virtual hardware switch using ports p1, p2, p3, and p4:

```
config system virtual-switch
  edit virt-sw-1
    set physical-switch sw0
      config port
        edit 1
          set port p1
          set speed <speed>
          set duplex { up | down}
        next
        edit 2
          set port p2
          set speed <speed>
          set duplex { up | down}
        end
        edit 3
          set port p3
          set speed <speed>
          set duplex { up | down}
        next
        edit 4
          set port p4
          set speed <speed>
          set duplex { up | down}
        end
```

FortiExplorer for iOS devices

You can use FortiExplorer for iOS to manage most FortiGate models running FortiOS 5.0 firmware from an iOS device (iPhone, iPad, or iPod Touch running iOS 5.0 or later). FortiExplorer is a free download from the Apple iOS App Store (App Store Link).

Connecting to and logging into a FortiGate unit

Use FortiExplorer for iOS by connecting your iOS device to any FortiGate USB port, using the USB cable that came with your iOS device. (Connect to any FortiGate USB-A port. There is no need to connect to the USB-B port required for the PC or Mac OS versions of FortiExplorer).

Start FortiExplorer on your iOS device and select *Setup* and log into the FortiGate unit using any administrator account user name and password.

After logging in, you can use FortiExplorer to change the firmware running on the FortiGate unit, configure network settings, and change general system settings. You also have one-step access to the configuration of each FortiGate interface.

Updating firmware and configuring network settings

Usually you would use FortiExplorer to upgrade firmware and configure network and basic settings. Then log into the web-based manager for more advanced configuration. However, you can select *Web* to connect directly to the FortiGate unit's web-based manager from your iOS device.

You can also select *Firmware* to view the available firmware versions for any FortiGate model and download new firmware and install it on your FortiGate unit.

Inter-VDOM links between NAT mode and Transparent mode VDOMs

FortiOS 5.0 supports inter-VDOM links between NAT and Transparent mode VDOMs. No special configuration is required and you can create an inter-VDOM link between NAT and Transparent mode VDOMs in the same way as creating an inter-VDOM link between two NAT mode VDOMs.

About inter-VDOM links between NAT and Transparent mode VDOMs

Inter-VDOM links between NAT and Transparent mode VDOMS can be useful for configurations where the NAT based VDOMs that share a common Internet service route, which can be routed through a Transparent VDOM that provides additional functionality, like common Security inspection, WAN optimization, explicit proxying and so on.

Other examples include:

- Performing SSL offloading in the Transparent mode VDOM and providing Internet access through a NAT mode VDOM.
- Applying WAN optimization in a Transparent mode VDOM and other security features in the NAT mode VDOM.
- Using a dedicated Transparent mode VDOM for the explicit web proxy in front of a NAT mode VDOM that applies other security features.
- An ISP configuration with multiple per-tenant NAT mode VDOMs all sharing a single Internet connection but where the ISP only presents a single routed subnet. Each tenant can then be assigned an IP from the subnet for their respective VDOM link interface while using a single physical port to connect to the ISP router.

Sniffer modes: one-armed and normal

FortiGate units can operate in one-arm sniffer mode or as a regular traffic sniffer. When the FortiGate unit has an interface dedicated to its exclusive use (one-arm sniffer mode), all traffic entering the interface is processed by the sniffer. The traffic is compared to the configured filters and data that doesn't match the filters is discarded. The selected Security profiles process the remaining traffic and log their findings. At the same time, the packets triggering the configured Security features are saved for later examination. After all examination of the traffic is complete, it is discarded. This continues until the configured maximum number of packets are saved, when the sniffer stops.

When the sniffer does not have an interface dedicated to its exclusive use, the traffic is examined by the sniffer, then processed normally by the FortiGate unit. That is, traffic is sniffed and can then leave the FortiGate unit depending on how it is configured. The sniffed interface traffic is examined for traffic matching the sniffer filters and matching packets are saved. Security features can not be used to limit the traffic the sniffer examines when not in one-armed mode. When the configured maximum number of packets is saved, the sniffer stops. The FortiGate unit continues to process network traffic as normal.

Configuring an interface to operate as a one-arm sniffer

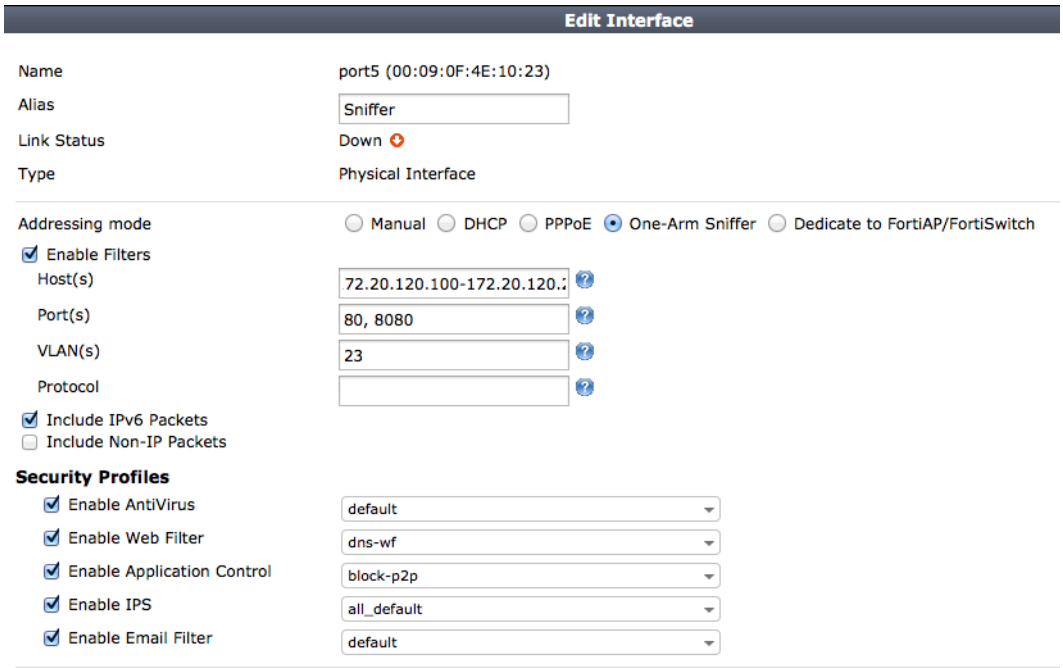
Connect the interface to the network to be analyzed. Go to *System* > *Network* > *Interfaces* and edit the interface and select *One-Arm Sniffer* and select *Apply*.

Configure the sniffer by selecting *Enable Filters* to filter traffic by IP address (host), address range, port number, VLANs and protocols. You can also configure the sniffer to *Include IPv6 Packets* and to *Include Non-IP Packets*.

Finally, under *Security Profiles* you can select Security profiles to apply to the sniffer.

Select *Apply* to save your changes.

Figure 97: Example one-arm sniffer configuration



Integrated switch fabric (ISF) access control list (ACL) short-cut path

On FortiGate models that include NP4 and XLR ports and an integrated switch fabric (for example, the FortiGate-3x40 and 3950/1 models), you can create an ISF ACL security policy that allows some traffic (for example, multicast traffic) to bypass security inspection, resulting in reduced CPN and NP4 processor load.

This feature is only available in Transparent mode and only between port pairs.

Traffic accepted and forwarded by an ISF policy is not subject to security inspection. Normally, you should only create ISF policies for traffic that you consider very low risk.

Use the following command to add an ISF ACL shortcut policy:

```
config firewall isf-acl
  config port-pair-1
    edit 1
      set type binary
      set ingressport <port1 | port2>
      set offset
      set length
      set matchpattern <patter in hex>
      set action <bypass|block>
    edit 2
      set type 5-tuple
      set srcaddr: a.b.c.d/32
      set dstaddr 239.A.A.a/32
      set proto UDP
      set port XXX
      set action <bypass|block>
  end
```

Generalized TTL Security Mechanism (GTSM) support

Generalized TTL Security Mechanism (GTSM), defined in RFC 5082, prevents attacks based on forged protocol packets sent from outside the network.

In IP packets, the TTL (time-to-live) value sets the maximum number of routers the packet can pass through to reach its destination. Each router decrements the TTL value and the packet is discarded if TTL reaches zero before the packet reaches its destination. In IPv6, TTL is called Hop Limit.

Most protocol-related packets pass between adjacent routers, so the TTL value at the destination is within a predictable range. TTL is difficult to spoof, especially the value of 255 which occurs if the sender is directly connected to the destination router.

On the FortiGate firewall, you can define TTL policies that specify the acceptable TTL range for a particular packet source, destination and service. You do this using the new `config firewall ttl-policy` command.

Use the following command to add a TTL policy that sets the TTL range to from 20 to 30:

```
config firewall ttl-policy
  edit 0
    set srcintf port1
    set srcaddr example_net
    set service ALL
    set schedule always
    set ttl 20-30
  end
```

Firewall services

The CLI command `get fireall service predefined` command has been removed. All predefinied services have been moved to `{get | set} firewall service custom`.